Departamento de Informática

PROYECTO FIN DE CARRERA

BUSINESS CONTINUITY PLAN – CONCEPTOS TEORICOS Y SIMULACION PRACTICA

Autor: Samuel Pascual Martín

Titulación: Ingeniería Técnica en Informática de Gestión

Tutor: Miguel Ángel Ramos

Leganés, Octubre de 2015

Título: BUSINESS CONTINUITY PLAN – CONCEPTOS TEORICOS Y SIMULACIÓN PRÁCTICA
Autor: Samuel Pascual
Director: Miguel Ángel Ramos González

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 20__ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

A D. Miguel Ángel Ramos, el tutor de este proyecto, sin cuya guía y ayuda no hubiera sido posible.

A mis padres.

A M.

Gracias.

Resumen

El presente Proyecto de Fin de Carrera pretende realizar una aproximación tanto teórica como práctica a los Planes de Continuidad de Negocio empresariales.

En primer lugar el Proyecto plantea la necesidad para las Empresas de disponer de planes formales de continuidad y recuperación, estructurados y elaborados siguiendo una metodología determinada. Esto es de gran importancia debido al enorme impacto que pudiera tener la ocurrencia de un desastre para cualquier Compañía.

A continuación el Proyecto describe teóricamente varios conceptos necesarios sobre la Continuidad de los negocios. Se proporcionan no sólo definiciones, si no también pautas y recomendaciones para poder elaborar estructuradamente un Plan de Continuidad desde la fase inicial, desde la realidad empresarial de hoy en día.

Más adelante se aplican los conceptos descritos en la parte teórica a una situación simulada, desarrollada sobre una empresa ficticia de tamaño medio. En esta parte se van aplicando paso por paso todos los apartados teóricos descritos en la parte anterior, indicando cómo se aplicarían sobre el ejemplo concreto. De esta manera puede ponerse al lector en una situación de aproximación a la realidad, y apreciarse cómo las características de cada empresa darán como resultado un Plan de Continuidad distinto.

Por último, y como anexos, se han incluido los documentos reales del Plan de Continuidad que daría como resultado la implantación del Proyecto en la compañía simulada.

Palabras clave:

Plan de Continuidad de Negocio, BCP, Business Continuity Plan, Recuperación de Negocio, Simulación práctica BCP

Abstract

This Final Project intends to be an approach, both from theoretical and practical perspective, to corporate Business Continuity Plans.

In a first stage, this Project shows the need that the corporations have to maintain formal continuity and recovery plans, which are made and structured following a methodology. This matter has great importance nowadays, due to the big impact that a disaster could have to any Company.

Next, this Project describes theoretically some concepts in business continuity. There are not just definitions provided, but also guidelines and recommendations to develop a Business Continuity Plan from its initial stage, taking in to account the reality of the corporations nowadays.

In the next chapter, some of the concepts described in the theoretical stage are now applied to a simulated case, of a medium-size company. In this part of the project all the concepts provided are applied step by step over this simulated company. In this way, the reader can approach a more real situation, and realize about that the different characteristics of each company will provide a different Business Continuity Plan.

Finally, are included as annexes the real BCP documents which would result of the implementation of the Project in the simulated company.

Keywords:

BCP, Business Continuity Plan, Business recovery, BCP Practical simulation

Índice General

Índice de Figuras

Índice de Tablas

Capítulo 1.- Introducción y objetivos

1.1.- Introducción

A día de hoy gran cantidad de entidades ofrecen a sus clientes muy diversos productos y servicios con el apoyo de las Tecnologías de la Información. La importancia de estos servicios tecnológicos para las organizaciones aumenta día a día, así como también lo hace la dependencia de las mismas hacia estos procesos.

A pesar de su importancia, dichos elementos se encuentran permanentemente en riesgo, y las organizaciones están continuamente expuestas a fallos o amenazas que pueden ocasionar una paralización de sus sistemas básicos. Esta paralización podría poner en peligro la prestación de los citados servicios y productos a sus clientes, llegando incluso a afectar la propia continuidad de las compañías.

Se hace indispensable por tanto, en el mundo empresarial de hoy en día, disponer de un plan que sea capaz de gestionar eficientemente los posibles incidentes que pudieran acontecer, para que el daño que dichos incidentes puedan ocasionar al negocio sea el mínimo posible. Este plan proporcionará las pautas para, a partir de un análisis previo de los sistemas y procesos de la entidad, asegurar la pronta recuperación de los mismos con el objetivo de minimizar el impacto tanto al servicio proporcionado a los clientes como a la imagen corporativa tras el incidente.

El Proyecto Fin de Carrera a continuación realiza un análisis pormenorizado de en qué consiste un Plan de Continuidad de Negocio y cómo puede implementarse en una empresa actualmente.

1.2.- Objetivos

Este Proyecto Fin de Carrera tiene como intención la consecución de los siguientes objetivos:

- Mostrar la necesidad para las empresas de disponer de un plan de continuidad de negocio formal que estructure y describa una estrategia de continuidad.

- Definir y explicar teóricamente determinados conceptos relacionados con la continuidad de los negocios.

- Proporcionar unas herramientas, basadas en una simulación práctica, para ayudar al lector a elaborar un Plan de Continuidad que posibilite tanto la prevención de riesgos en una compañía, como la recuperación del funcionamiento de procesos críticos de la misma en caso de la ocurrencia de un desastre.

1.3.- Fases del desarrollo

El desarrollo del Proyecto Fin de Carrera a continuación se ha realizado en las siguientes fases:

- Inicialmente, se plantea la necesidad de las empresas de disponer de un plan de continuidad, se realizan las definiciones iniciales necesarias, y se describen, desde una perspectiva teórica, los pasos necesarios para elaborar un plan de continuidad.

- En una segunda fase, se intentan aplicar de forma práctica los conceptos teóricos explicados en la primera fase. Para ello se define una compañía simulada, SPBCP Consulting S.A., y se va implementando todo un Plan de Continuidad a partir de la hipotética situación de un mandato de la Dirección General de la citada compañía simulada.

- La tercera fase se corresponde con el diseño de la planificación utilizando un Diagrama de Gantt, así como la realización de un presupuesto de implantación para la situación simulada en la segunda fase del proyecto.

- Por último, y como anexos, se muestran los documentos definitivos que resultarían de la implantación del Plan de Continuidad en la compañía simulada SPBCP Consulting S.A., para proporcionar al lector un ejemplo de documentación en el desarrollo de un plan de continuidad.

1.4.- Estructura de la memoria

Para facilitar la lectura de la memoria, se incluye a continuación un breve resumen de cada capítulo:

- Capítulo 1: Introducción y Objetivos

Este capítulo realiza una breve introducción inicial a los Planes de Continuidad de Negocio, presenta los objetivos que persigue el Proyecto de Fin de Carrera, y explica las fases de desarrollo del proyecto.

- Capítulo 2: Business Continuity Plan: Conceptos Teóricos

El capítulo 2 ofrece una aproximación teórica al concepto del Plan de Continuidad de Negocio, y desarrolla teóricamente las fases necesarias para la implantación de un plan de este tipo a nivel corporativo.

- Capítulo 3: Business Continuity Plan: Simulación Práctica

Este capítulo desarrolla el modelo teórico de implantación de un plan de continuidad presentado en el capítulo 2 sobre una simulación práctica. La simulación propone la cuestión de la implementación de un Plan de Continuidad para una compañía ficticia ubicada en Madrid, desde el momento inicial hasta la implantación completa del plan.

- Capítulo 4: Planificación Y Presupuesto

El capítulo 4 describe la planificación del proyecto de implantación mediante un diagrama de Gantt, y detalla el presupuesto para llevar a cabo dicha implantación.

- Capítulo 5: Conclusiones

El capítulo 5 ofrece las conclusiones al Proyecto Fin de Carrera, así como sugerencias para futuros trabajos a partir de este PFC.

- Capítulo 6: Glosario

- Capítulo 7: Referencias

- Capítulo 8: Bibliografía

- ANEXOS

Se han recogido como Anexos (del I al V) los documentos finales que formarían parte del Plan de Continuidad de Negocio de la empresa simulada en el Capítulo 3.

CAPITULO 2.- BUSINESS CONTINUITY PLAN: Conceptos teóricos

2.1.- Definición de BCP

Según la obra Planes de Contingencia: La Continuidad del negocio en las organizaciones, de Juan Gaspar Martínez, se denomina Plan de Continuidad de Negocio al "… conjunto de estrategias y procedimientos preventivos y reactivos que permitan un rápido retorno a una situación suficientemente normalizada para que la actividad de la organización recupere un nivel aceptable después de una interrupción no prevista de sus sistemas de información, para más tarde volver a la situación normal de funcionamiento" [PDC-DEF]

Otra acepción, según la Wikipedia, de Plan de Continuidad de Negocio, es la siguiente: "Un plan de continuidad del negocio (o sus siglas en inglés, BCP, por *Business Continuity Plan*) es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre". [WIK-BCP]

A grandes rasgos, podríamos definir el Plan de Continuidad de Negocio de una Compañía como el conjunto de tareas de análisis, planificación, implantación, documentación y mantenimiento que faciliten la ejecución de las actuaciones necesarias para lograr el restablecimiento eficiente de las funciones de una Empresa, si se diera el caso de que algún incidente inesperado pusiera en peligro el funcionamiento normal de la misma.

Entre los citados incidentes se encontraría cualquier evento que pudiera producir la interrupción de la actividad normal de la Compañía, como pudieran ser cortes prolongados en el suministro eléctrico, virus informáticos, fallos humanos, incendios, terremotos, inundaciones, terrorismo, pandemias…

Ante la necesidad de disponer de un plan fiable que sea capaz de mitigar los efectos adversos que pudieran producir estos eventos si tuvieran lugar, surge el Business Continuity Plan como un conjunto de análisis, medidas activas y preventivas, pruebas y documentos, destinado a guiar paso por paso al personal a cargo hasta la restauración de la actividad total de la Compañía, en un periodo de tiempo que afecte lo menos posible al cumplimiento de los compromisos y contratos de la misma con sus clientes.

Así, podemos establecer los siguientes objetivos principales para cualquier Plan de Continuidad de Negocio:

- Analizar la estructura e infraestructura de la Compañía con sentido crítico, para conocer sus procesos y sistemas, constatando los puntos débiles que éstos puedan tener.
- Identificar los riesgos que pueden afectar a la Organización, y el impacto que pueda tener cada uno de ellos en caso de materializarse.
- Establecer una serie de medidas preventivas y estrategias de recuperación para minimizar el impacto en la Compañía en caso de contingencia.
- Disponer de una guía para que el personal a cargo de la continuidad del negocio pueda restaurar los sistemas y procesos de la manera más eficientemente posible, incluso en un entorno de gran presión como el que pudiera suponer un desastre.
- Salvaguardar los intereses de la misma Compañía, así como de sus clientes y accionistas, velando por la imagen de la organización y por el cumplimiento de los compromisos adquiridos a pesar del desastre.

La importancia de disponer de un Plan de Continuidad es crítica en las organizaciones actuales, donde tanto los Sistemas de Información como los datos que tratan tienen un papel fundamental para el funcionamiento de las mismas. El hecho de poder o no contar con una estrategia donde se especifique la secuencia de acciones a tomar en caso de desastre, y que incluya aspectos como los procesos críticos a recuperar, el personal involucrado, la infraestructura necesaria, etc, puede ser tan significativo como para suponer la diferencia entre la desaparición de nuestra Compañía o la continuidad de la misma. Esto es así hasta el punto que, de las empresas afectadas por un desastre, únicamente un 6% de las que han sufrido pérdida irreversible de sus ficheros automatizados permanecerá a largo plazo, mientras que el 51% cierra sus puertas en menos de dos años [BACK-HOF].

2.2.- Elaboración del BCP

Dada la extensión de los aspectos a tener en cuenta a la hora de la confección del Plan, este debe estructurarse por fases separadas y bien definidas para evitar dejar de incluir en el mismo aspectos críticos que pudieran no tenerse en cuenta a la hora de aplicarlo.

La elaboración del BCP implica en primer lugar un análisis pormenorizado de toda la Compañía y sus procesos. Ya desde esta fase se debe contar con el apoyo de la Dirección y de todos los Departamentos. Tengamos en cuenta que será un proyecto al que la Empresa destinará tiempo y recursos sin un retorno de la inversión evidente a corto plazo, con lo que contar con este entendimiento y apoyo desde el primer momento será básico para que el Plan pueda confeccionarse.

Una vez analizada la situación actual, se procederá a diseñar el Plan propiamente dicho, generando la documentación correspondiente. Esta documentación será la que servirá de referencia en caso de que hubiera necesidad de aplicar el Plan en el futuro.

Pero aun estando ya generado el Plan, el trabajo no ha terminado: es necesario realizar pruebas y simulacros para comprobar que las acciones diseñadas en el mismo son de utilidad y tienen sentido, y también será necesario revisarlo periódicamente para incluir los cambios que se pudieran haber producido desde la situación anterior al momento actual.

En los apartados a continuación se detallan por orden las diferentes fases que se pueden seguir a la hora de elaborar un Business Continuity Plan.

2.3.- Planificación del Proyecto

Los primeros pasos a la hora de realizar cualquier proyecto son la exposición de la motivación del mismo a partir de la situación existente, el establecimiento de unos objetivos generales, y la explicación de los resultados esperables a la finalización del mismo.

Este informe inicial se presentará a la Dirección para exponer la necesidad de realizar el Plan de Continuidad, buscando la aprobación y el apoyo de la misma para llevarlo a cabo.

Esta primera fase es muy importante para el Plan de Continuidad, ya que la Compañía debe respaldar tanto organizativa como financieramente el mismo, a pesar de ser un proyecto que no tiene un retorno de la inversión a corto plazo. En este informe habrá que exponer claramente, por tanto, los beneficios de disponer de un BCP, así como los riesgos de no contar con él, para que la Dirección pueda tomar una decisión respecto al proyecto conociendo todas las implicaciones y el coste estimado de su implantación.

2.4.- Análisis de la Compañía

Una vez que el proyecto haya sido aprobado por la Dirección, procederemos a realizar un análisis de la situación actual de la Compañía. En este análisis se deben describir las características principales de la Empresa (ámbito del negocio, sedes, organización, procesos, sistemas), que tendremos en cuenta a lo largo de todo el Proyecto. El análisis preliminar nos proporcionará una idea clara inicial de la situación actual de la Empresa en relación con los siguientes aspectos:

- Infraestructura de la Compañía
- Personal responsable de cada área
- Objetivos del negocio
- Sistemas actuales
- Criticidad de los procesos de la Empresa
- Planes de Continuidad actuales

El conocimiento previo de todos estos aspectos será de gran utilidad para establecer una fotografía de la situación actual de la Empresa, que sirva de base para el desarrollo posterior del Proyecto.

2.5.- Análisis de Riesgos

En esta fase se deberán identificar, enumerar y evaluar los distintos riesgos y vulnerabilidades que pueden afectar a la Compañía, y ordenarlos de acuerdo a su probabilidad de ocurrencia e impacto en el desarrollo normal de las funciones del negocio.

Los riesgos a los que se enfrenta cada compañía pueden resultar muy variados, dependiendo de la naturaleza de su negocio (no afrontan los mismos riesgos una floristería que una plataforma petrolífera, por ejemplo), de la localización de sus instalaciones (el riesgo de inundación, por ejemplo, es superior en localizaciones próximas a ríos o mares, o ubicadas en emplazamientos naturales de rieras), o de cualquier otro factor específico de la Compañía. Por tanto, en esta fase tendremos en cuenta tanto la incidencia como el impacto de todos estos factores propios de la peculiaridad de la Empresa cliente a la hora de desarrollar el análisis de los riesgos.

Existen metodologías muy diversas para el análisis de riesgos, ya que éste no sólo se aplica a la disciplina de la Continuidad de Negocio, entre las que cabe destacar las siguientes:

- MAGERIT – "Metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica". Es el método actual de aplicación en la Administración Pública Española. [MAGE-HTP]
- OCTAVE – Técnica de evaluación de riesgos diseñado por la Oficina de Patentes de EE.UU.
- CRAMM – "CRAMM es la metodología de análisis de riesgos desarrollada por la Agencia Central de Comunicación y Telecomunicación del gobierno británico"

Sin embargo, todas ellas tienen puntos comunes, que son los que deberemos contemplar siempre que hagamos un Análisis de Riesgos, sea cual sea el método que utilicemos. Estos puntos comunes y que podemos utilizar para realizar un análisis de riesgos fiable y completo son los siguientes:

- Enumeración de los activos críticos de la Compañía
- Identificación de las vulnerabilidades asociadas a dichos activos
- Valoración de las posibles amenazas junto con su probabilidad de ocurrencia
- Determinación del impacto que puede existir

El análisis de riesgos es una parte importante en la elaboración del BCP, ya que proporcionará una visión de las posibles amenazas y contingencias que podrían ocurrir. Será a partir de estos riesgos de los que se deduzcan las posibles soluciones, tanto reactivas como proactivas, para mitigarlos.

2.6.- Análisis de Impacto al Negocio

Una vez que tenemos una idea de la estructura y el funcionamiento de la Compañía, y de los riesgos que pueden poner en peligro el funcionamiento de la misma, procederemos a integrar la información de ambos análisis en lo que se denomina Análisis de Impacto al Negocio (BIA, por sus siglas en inglés).

No hay que confundir el análisis de los riesgos realizado en el apartado anterior, con el Análisis de Impacto al Negocio. El primero de ellos determina los sucesos que podrían causar la interrupción del funcionamiento normal de la Compañía (caída de los sistemas, de las comunicaciones, corte de suministro eléctrico, etc), mientras que el BIA indica los efectos que provocaría esta interrupción del sistema sobre los procesos de negocio si el evento llegara a suceder.

Actualmente no existe un estándar para la realización del BIA. Sin embargo en cualquier Análisis de Impacto deben recogerse unos elementos comunes de información y conceptos básicos, que darán una idea de cómo los riesgos pueden afectar a los procesos críticos de la Compañía. Así, al realizar un Análisis de Impacto, deben tenerse en cuenta al menos los siguientes aspectos:

- Proceso crítico: Nombre y descripción del proceso crítico a analizar.
- Prioridad del proceso: Valor de prioridad que se asigna al proceso en caso de ser necesario el restablecimiento del mismo.
- Tiempo Máximo de Interrupción: Tiempo máximo en el que la Empresa podría prescindir del proceso con un impacto asumible.
- Tiempo de Recuperación Objetivo: Es el tiempo necesario esperado para la recuperación del proceso en caso de interrupción.
- Recuento de personal: Número de personal a tiempo completo dedicado al proceso.
- Impacto al negocio: Valoración del impacto causado al negocio en cada fase. Este impacto puede ser de muy distintas magnitudes, como económico, legal, contractual, de reputación, o incluso una mezcla de varias de ellas.

Como normal general se priorizará la recuperación del proceso que suponga mayor impacto a cada área de negocio, para que de esta forma la pérdida asociadas al cese del servicio sea lo menor posible.

Tras efectuar el análisis anterior los resultados del BIA deberán ser puestos en común con la Dirección de las distintas áreas de la Empresa, para verificar si el posible impacto al negocio y sus consecuencias (económicas, operativas, de reputación, de cumplimientos contractuales con clientes, legales, etc) se han estimado de manera realista.

Tanto la confección como la revisión por la Dirección de este punto son importantes, ya que una mala evaluación del impacto nos podría hacer cometer errores en el caso de que hubiera que aplicar el Plan. Así podríamos recuperar procesos que no son críticos antes que otros que sí lo son, o no recuperar completamente procesos cuya importancia sí hubiera sido bien estimada, pero no su naturaleza.

2.7.- Estrategia del BCP

Llegados a este punto ya dispondremos de una imagen fiel y concisa de la estructura de la Compañía, los posibles riesgos que puede afrontar y el impacto que puede tener el negocio en caso de que alguno de estos riesgos se materializase. Es hora, por tanto, de comenzar a desarrollar la estrategia de recuperación que seguiremos para que el perjuicio que se pudiera ocasionar sea mitigado cuanto antes.

A la hora de hablar de continuidad tendremos en cuenta dos estrategias principales: la recuperación propiamente dicha, en la que nos basaremos para paliar los daños cuanto antes si el desastre llegara a suceder, y la prevención, que, si se aplica adecuadamente, minimizará el impacto y hará mucho más eficiente la recuperación en sí.

Estas dos estrategias no son excluyentes entre sí. De hecho, una buena estrategia de prevención facilitará en grado sumo la recuperación, si finalmente tuviera que llevarse a cabo.

- Prevención

Según la definición del Diccionario de la R.A.E. de la Lengua, el término Prevención se define como la "Preparación y disposición que se hace anticipadamente para evitar un riesgo o ejecutar algo" [PREV-RAE]. Como se aprecia, la idea de evitar el riesgo está implícito en la propia definición de prevención.

Este concepto es, por tanto, muy conveniente para ser aplicado en la estrategia de desarrollo del Plan de Continuidad. Esta estrategia de prevención se basa en aplicar a la infraestructura de la Compañía, a la forma diaria de trabajo y a las futuras decisiones estratégicas la concepción de que los riesgos existen, para adoptar medidas preventivas que los minimicen.

Entre estas medidas preventivas pueden encontrarse algunas como las siguientes:

- Planificar unas instalaciones donde la seguridad esté siempre presente: disponer de sistemas contra incendios, mantener limpios los espacios de trabajo, revisar periódicamente las instalaciones eléctricas, etc.
- Mantener inventarios actualizados de los Sistemas de Información de la Compañía
- Disponer de conexiones de datos redundantes.
- Dotar a las infraestructuras de sistemas de alimentación ininterrumpida para minimizar el impacto que pudiera provocar un corte de suministro eléctrico.
- Realizar copias de seguridad periódicas de los datos almacenados en la Compañía.
- Realizar copias de seguridad de la configuración de los sistemas de la Compañía.
- Disponer de una salvaguarda de los sistemas y los datos fuera de las instalaciones de la Compañía.

- Los sistemas de la Compañía deben disponer de medidas de seguridad adecuadas: sistemas operativos actualizados, antivirus actualizados, seguridad perimetral…
- Dotar de teléfonos móviles y posibilidad de conexión segura desde el exterior de las oficinas (VPNs) al personal que gestiona los procesos críticos del negocio.
- Contemplar la posibilidad de utilizar equipos portátiles, que disponen de batería propia y pueden ser utilizados fuera de las instalaciones de la Compañía en caso de que éstas no estén disponibles.
- Contar con seguros en vigor que cubran los activos de la Compañía en caso de rotura o desastre.
- Formar a los empleados periódicamente sobre las políticas de seguridad y prácticas de buen uso de la Compañía para conseguir minimizar en lo posible el error humano.

Nótese que el hecho de disponer de medidas preventivas como las mencionadas, implementadas de forma natural en la Compañía, disminuirá en gran medida el impacto que puedan producir muchos de los riesgos. En realidad, las medidas preventivas están operativas continuamente, ya que forman parte de la infraestructura habitual de la Organización, y evitan por sí mismas que el BCP tenga que ser activado al producirse un riesgo ya previsto.

▪ Recuperación

A pesar de contar con unas medidas preventivas adecuadas, puede darse el caso de que finalmente la interrupción del servicio se produzca. Por tanto, debemos contar con unas estrategias de recuperación adecuadas para poder afrontar esta situación lo más eficientemente y con el mínimo impacto posible para la Organización.

Independientemente de cuáles sean estas estrategias concretas de recuperación elegidas, todas ellas deben contemplar cómo llevar a cabo los siguientes aspectos:

- Organización de los Recursos Humanos para poder desempeñar los procesos críticos de la Compañía. En esta primera fase inicial la Dirección y el Departamento de IT desempeñan un papel fundamental para la recuperación.
- Habilitación de unas instalaciones alternativas donde poder llevar a cabo las funciones críticas de la Empresa, en caso de que las instalaciones habituales se hayan visto afectadas.
- Establecimiento de unas infraestructuras básicas sobre las que iniciar nuevamente las Comunicaciones y Sistemas necesarios.
- Restablecimiento de los Sistemas necesarios para poder desempeñar los procesos básicos.
- Recuperación de los datos corporativos a partir de las copias de seguridad.

Una vez que estas primeras acciones básicas han sido ejecutadas, siempre siguiendo la guía del BCP, cimentaremos sobre las mismas el resto de la recuperación, para que la Compañía pueda, en el mínimo tiempo posible, volver a la situación anterior al desastre.

2.8.- Desarrollo del BCP

Estando definidas las estrategias de prevención y recuperación, se plantea la cuestión de cómo implementar dichas estrategias si el desastre llegara a producirse, y fuera necesario ejecutar el BCP.

Así, si finalmente el Plan de Continuidad debe ejecutarse, se contemplarán los siguientes aspectos a la hora de desarrollarlo:

- Medir en qué momento debe empezar a aplicarse el Plan. Normalmente será una situación concreta o límite previamente definida la que haga que el Plan comience a llevarse a cabo.
- Las personas indicadas, definidas en el BCP, comenzarán a tomar las decisiones concretas para la activación, ejecución y gestión del Plan.
- Se dispondrán los recursos adecuados para la ejecución del Plan.
- Comenzarán a implementarse las estrategias de recuperación, para dotar de una infraestructura básica a la Compañía en un corto plazo de tiempo.
- Se recuperarán los procesos críticos de la Empresa, de acuerdo con la prioridad definida en el BCP.
- Durante todo este proceso se realizarán las comunicaciones pertinentes a los medios, clientes y proveedores, para no dañar la imagen de la Organización.

El Desarrollo inicial del Plan de Continuidad será de gran ayuda para gestionar la situación inicial de crisis, los complicados primeros momentos de nerviosismo y desconcierto que afrontará la Organización en esta situación. Sin embargo, la finalidad última del Plan de Continuidad de Negocio es restaurar la situación de la Compañía a la existente previa a la situación de crisis. El correcto desarrollo del Plan de Continuidad desde el primer momento, aparte de gestionar la situación inicial, sentará las bases para la recuperación definitiva de la Compañía con el mínimo impacto posible.

2.9.- Documentación del Plan

Como resultado de la elaboración del BCP se obtendrán diversos documentos que recojan toda la información y los procedimientos analizados y establecidos en las distintas fases del Plan de Continuidad. Esta documentación es de gran importancia, ya que servirá como guía en caso de ser necesaria la aplicación del mismo.

Los documentos que se obtendrán tras el desarrollo del Plan de Continuidad son, como mínimo, los siguientes:

- BIA (Business Impact Analysis): Documento que recoge el análisis de los posibles riesgos que pueden afectar a los sistemas y procesos de la Compañía. Este documento especifica el posible riesgo que se afronta, detalla los sistemas y procesos afectados si el riesgo se convirtiera en desastre, y cuantifica el impacto para cada sistema o proceso que se viera afectado. En este documento normalmente se incluye el Análisis de Riesgos realizado previamente al BIA.

- Plan de Crisis: Este documento contiene la información necesaria para la gestión de la crisis desde los momentos iniciales, indicando aspectos tales como el personal a cargo de la recuperación, los contactos necesarios para la gestión de incidencias, los tiempos de resolución de incidencias, etc. Es de gran importancia, ya que indica los pasos a seguir en primer lugar cuando el desastre ha ocurrido, lo que es de enorme utilidad en una situación de posible desconcierto y nerviosismo.

- DRP (Disaster Recovery Plan): El Disaster Recovery Plan es el documento que detalla los procesos necesarios para proteger y recuperar la infraestructura IT en caso de desastre. Este documento debe ser creado y mantenido por el Departamento de IT, y es básico dentro del BCP debido al papel fundamental que juegan actualmente las Tecnologías de la Información en las empresas.

- BCP (Business Continuity Plan): El BCP propiamente dicho es el documento final que servirá de guía para la prevención y recuperación de la Compañía en caso de desastre. No sólo sintetiza y recoge todos los documentos anteriores, que forma parte del plan, sino que también incluye información específica sobre el proceso completo de recuperación, incluyendo toda la estrategia de continuidad de la Compañía.

- Plan de mantenimiento y pruebas: Este documento detalla las políticas de mantenimiento del BCP, e incluye las pruebas a realizar periódicamente para asegurar que el Plan es de utilidad y está correctamente planteado si tiene que ejecutarse en algún momento.

- Documentación de formación a empleados: Podemos añadir también como documento resultante del desarrollo del Plan la documentación necesaria para la formación de los empleados en cuanto a la Continuidad de la Compañía. Esta documentación puede ser simplemente una pequeña guía,

pero al menos explicará por qué es importante la continuidad, y detallará las medidas preventivas que todos los empleados deben adoptar para minimizar los riesgos que afronta la Empresa.

2.10.- Ensayos Y Pruebas del BCP

Una vez que el BCP ha sido desarrollado y documentado ya se puede entender que la Compañía dispone de un Plan de Continuidad del Negocio que prevé y gestiona la ocurrencia de una disrupción del mismo. Sin embargo en este momento se dispone de una documentación teórica que ha sido analizada, desarrollada y estudiada, pero que nunca se ha aplicado en una situación real.

Es obvio que, por mucho que una situación se haya analizado sobre el papel, las contingencias que acontecen en una situación real no son comparables a su planificación teórica. Si la situación crítica finalmente tuviera lugar no sería extraño que pudieran ocurrir determinados imprevistos, como ocurrencia de riesgos adicionales, reacciones no previstas del personal implicado, fallo de algunas de las medidas de prevención descritas en el BCP, fallo de alguna de las medidas de recuperación, etc.

Para mitigar en la medida de lo posible estas situaciones imprevistas se hace necesario el desarrollo de un plan de ensayos y pruebas que pongan en práctica los conceptos teóricos analizados y definidos en el BCP. Estas pruebas no podrán ser completamente reales, ya que no podemos crear ni simular totalmente un escenario que nos lleve a poner en riesgo la continuidad del negocio con el propio ensayo, pero sí podemos plantear una situación que el equipo de contingencia pueda afrontar, al menos de forma simulada.

Estos ensayos consistirán normalmente en el planteamiento de una situación de riesgo al equipo encargado de la recuperación, que se encontrará reunido. Este equipo deberá intentar aplicar el Plan de Contingencia, afrontando y solucionando todas las situaciones que aparezcan en la prueba. Como resultado se obtendrá no sólo una prueba del BCP, con posibles puntos a replantear, mejorar o actualizar, sino también una experiencia valiosa para el equipo de contingencia, que será de utilidad si finalmente la desgracia llegara a producirse.

2.11.- Mantenimiento del BCP

Para poder conseguir de una forma eficiente el objetivo final de nuestro Plan de Continuidad, que no es otro que la recuperación de los procesos de la Compañía en caso de desastre, tenemos que asegurar que la imagen de la misma que refleja dicho Plan esté actualizada y sea fiel a la situación real en cada momento.

Se ha de tener en cuenta que un BCP desactualizado puede contener errores que nos hagan perder tiempo a la hora de la posible recuperación, tales como disponer de datos de contacto obsoletos, referenciar a personas que ya no pertenecen a la Compañía, no detallar procesos críticos de nueva creación, etcétera. Estas pérdidas de tiempo y situaciones imprevistas pueden ser fácilmente evitadas mediante unas políticas de mantenimiento adecuadas para nuestro plan de continuidad.

En general, una política de mantenimiento adecuada para el Plan especificará ciertas revisiones periódicas (anuales o bianuales, por ejemplo), actualizaciones del mismo cuando se produzcan cambios en la estructura de la Compañía, o también cuando haya acontecido una situación que haya provocado la ejecución del BCP. Realizando estos mantenimientos nos aseguraremos de que siempre se dispone de un Plan adecuado a la situación actual de la Empresa.

3.- BUSINESS CONTINUITY PLAN: Simulación Práctica

A continuación se expone una simulación de cómo se desarrollaría un proyecto de implantación de un Plan de Continuidad de Negocio, a partir de los conceptos teóricos del apartado anterior. El proyecto se llevará a cabo en una empresa ficticia, que se describe en el apartado a continuación. Algunos datos como localizaciones, edificios, mapas, proveedores, etc. pueden ser verídicos (aunque la simulación esté basada en una compañía ficticia). No obstante, la información que aquí se recoja siempre será de dominio público y hallable en Internet.

El proyecto se va a desarrollar desde la perspectiva del Responsable de un hipotético Departamento de Sistemas y Seguridad, que tenga a su cargo tanto la seguridad como los sistemas de la Compañía.

3.1.- Descripción de la Compañía

La simulación de la implantación de un Plan de Continuidad en una Compañía se realizará para una empresa ficticia que llamaremos SPBCP Consulting. Se trata de una consultora informática de 160 empleados, con sede en Madrid. A continuación se detallan las características de esta empresa, que se utilizarán de aquí en adelante para realizar la simulación práctica.

- Razón social: SPBCP Consulting S.A.
- Domicilio social: C\Proción 7, 28023 Madrid
- Actividad de la Empresa: Consultoría informática
- Número de Empleados: 160
- Facturación: Superior a 14.000.000 € anuales

Dicha empresa cuenta con varios departamentos diferenciados:

- Operaciones, compuesto por 88 personas
- Proyectos, compuesto por 53 personas
- Ventas, compuesto por 6 personas
- RR.HH, compuesto por 4 personas
- Administración, compuesto por 4 personas
- Infraestructura, formado por 2 personas
- Sistemas y Seguridad, compuesto por 2 personas

Dentro de la plantilla de cada uno de estos Departamentos existe un Director, reportando cada uno de ellos al Director General de la Compañía.

A continuación se incluye un plano de las instalaciones de la Compañía.

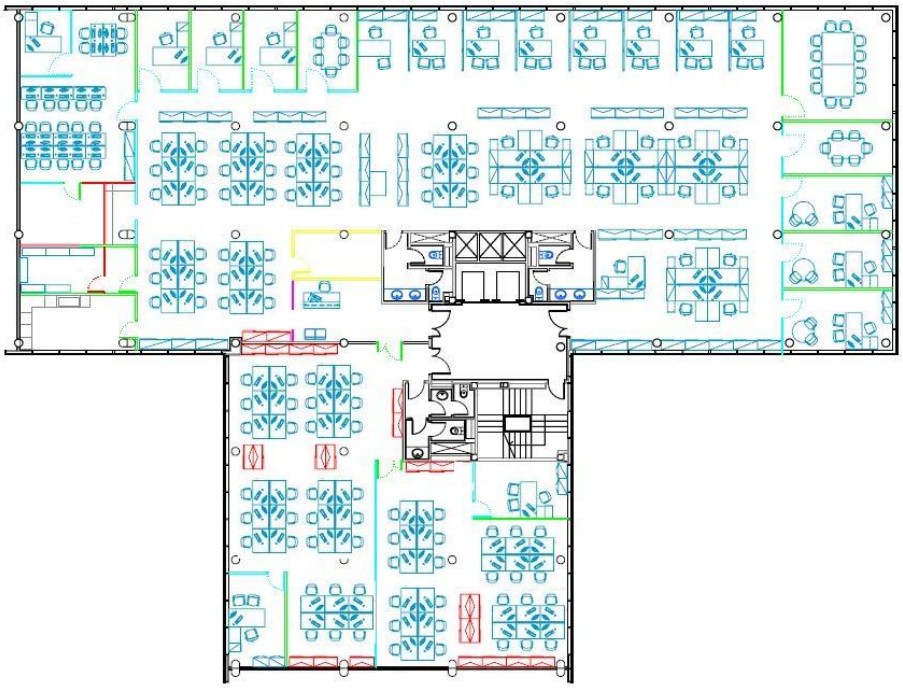


Figura 1.- Plano de las instalaciones de SPBCP Consulting S.A.

3.2.- Simulación de Planificación del Proyecto

Debido a la responsabilidad de la Compañía con sus Clientes y su masa social, así como al continuo crecimiento de la Empresa, en SPBCP Consulting se ha planteado la necesidad de contar con un Plan de Continuidad de Negocio actualizado que recoja todas las medidas y planes de acción necesarios para garantizar la continuidad de la Compañía en caso de enfrentarse a un desastre de cualquier tipo.

A partir de esta necesidad, la Dirección General ha encargado a la Dirección de Sistemas y Seguridad la ejecución de todas las acciones necesarias para que la Compañía cuente con un Plan de Continuidad de Negocio en un plazo de seis meses, y con un presupuesto máximo de 50.000 € asignados a este proyecto.

Siguiendo las instrucciones de la Dirección General, la Dirección de Sistemas y Seguridad elabora el Plan de Continuidad de Negocio para SPBCP Consulting, siguiendo los pasos detallados en los apartados a continuación.

Los documentos generados tras la elaboración del BCP se recogen en los anexos correspondientes.

3.3.- Simulación del Análisis de la Compañía

A partir del requerimiento de la Dirección General, la Dirección de Sistemas y Seguridad procederá en primer lugar a realizar un análisis de la situación actual de la Compañía.

El primer paso en este sentido será realizar una reunión con la Dirección de RR.HH. para obtener un organigrama de la Compañía que permita identificar a los máximos responsables de cada área. Será con dichos responsables con quienes se mantengan las primeras reuniones del proyecto, para plantearles la situación e involucrarles desde el primer momento en el Plan de Continuidad del Negocio. Este compromiso de todos los Departamentos será muy importante a lo largo de todo el ciclo de vida del BCP, ya que todas las áreas de la Compañía están relacionadas entre sí y ésta no puede funcionar sin una de sus partes.

En las reuniones preliminares con cada Departamento también se analizarán los planes de continuidad y políticas de recuperación actuales, su existencia, actualización, adaptación a la situación actual, etcétera. Se requerirá una copia de cada una de estas políticas y planes para tenerlos en cuenta en la elaboración del nuevo BCP.

De estas reuniones iniciales con todas las áreas de la Compañía debe obtenerse también como resultado la formación de un Equipo de Gestión de Continuidad. Este equipo, que estará formado preferiblemente por el máximo responsable de cada área y un delegado, será el encargado de ejecutar el Plan en caso de necesidad, y tomar las decisiones oportunas para la recuperación.

En la simulación se han realizado reuniones con los Directores de cada departamento de una hora de duración con cada uno, planteando la situación, recabando las escasas políticas actuales de continuidad que se encontraban por escrito para su adaptación al nuevo BCP, recogiendo sus opiniones y obteniendo el compromiso para su participación en el Proyecto. Posteriormente a estas reuniones se ha realizado una reunión adicional con todas las personas implicadas, coordinada por la Dirección General, donde se ha puesto toda la información en común, se ha establecido el Equipo de Gestión de Continuidad (representado en la Fig. X), y se ha tomado el compromiso por todas las partes de implantar el Plan de Continuidad de negocio.

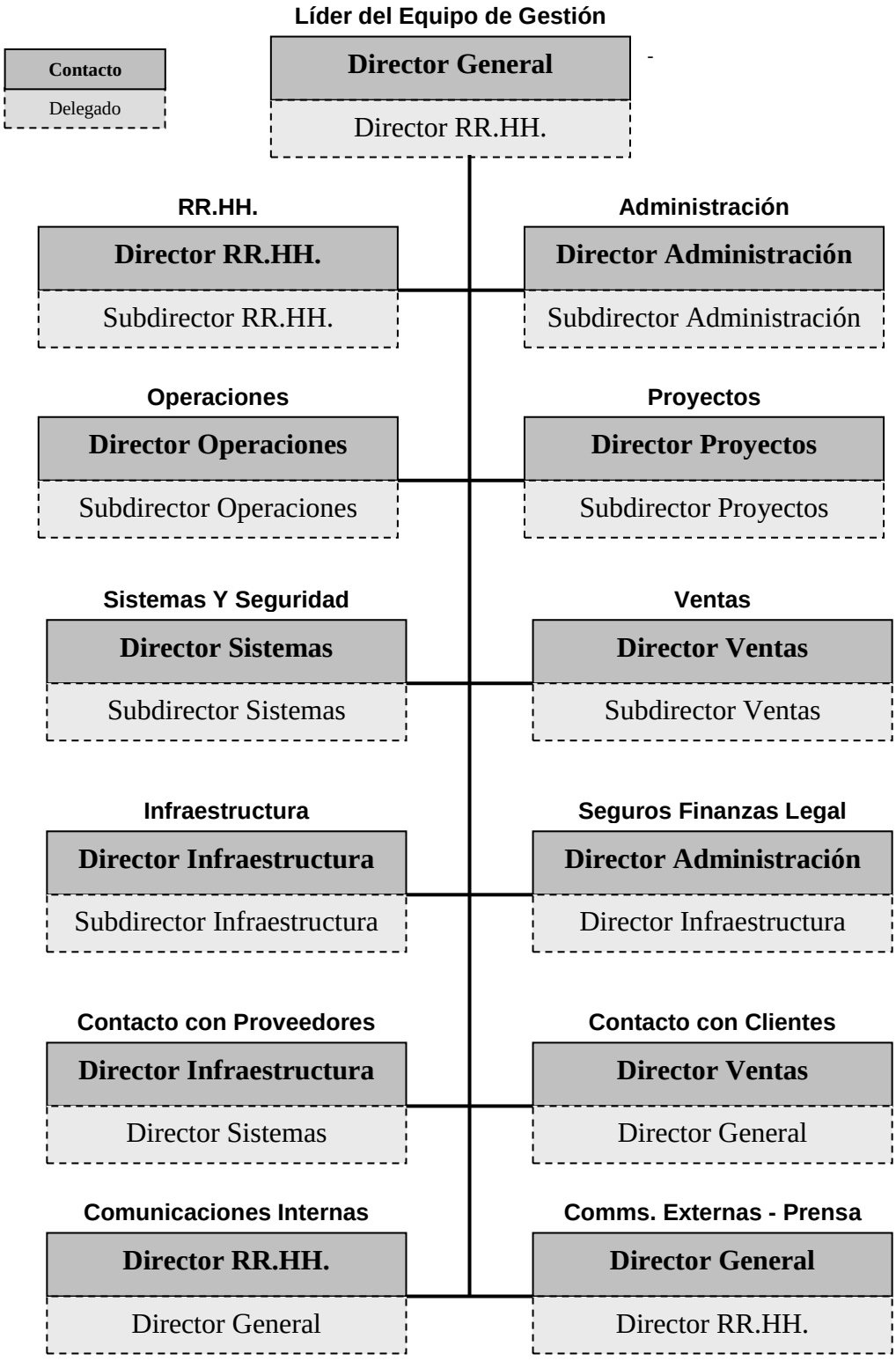


Figura 2 – Organigrama Equipo de Gestión de Continuidad.

Una vez que el Equipo de Gestión de Continuidad ha quedado establecido, se continuará con el análisis de la Compañía realizando reuniones adicionales con los responsables de cada área para establecer los procesos críticos de cada una de ellas, y los tiempos máximos de recuperación de cada proceso. Con esta información se obtendrá para cada departamento el tiempo máximo de inactividad admisible para que la disrupción no provoque un daño crítico al negocio, en relación con el personal de cada departamento.

Asimismo, en estas reuniones se indicará al Director de cada área la necesidad de contar con un Plan de Recuperación Departamental (PRD), donde cada departamento detalle sus procesos críticos y los pasos necesarios para recuperarlos en caso de desastre, así como el personal de cada departamento involucrado en dicha recuperación. Este Plan de Recuperación Departamental quedará bajo la responsabilidad de cada Departamento, pero podrán ser requeridos para ser consultados en caso de que fuera necesaria la ejecución del BCP.

En el ejemplo que se está simulando, tras haberse reunido con todos los Directores, se ha acordado que cada Departamento realizará su propio Plan de Recuperación Departamental, que conservará y mantendrá cada Director, y se han obtenido los detalles de cada proceso, estableciendo la criticidad de los mismos. Los procesos no considerados críticos por el Director de cada departamento se restablecerían en un término más largo, a elección de cada Departamento, no siendo incluidos en detalle en el BCP.

En la tabla a continuación se detallan, ordenados por su importancia, los procesos críticos a recuperar en relación con el personal necesario mínimo para ejecutar estos procesos. También se especifica el responsable del proceso y un teléfono de contacto.

DEPT. / PROCESO	CONTACTO	TELÉFONO	PERSONAL
Sistemas / Comms. + Datos	Director Sistemas	N. Teléfono	2
Operaciones / Proceso1	Director Operaciones	N. Teléfono	26
Operaciones / Proceso2	Director Operaciones	N. Teléfono	22
Operaciones / Proceso3	Director Operaciones	N. Teléfono	19
Proyectos / Proceso1	Director Proyectos	N. Teléfono	21
Proyectos / Proceso2	Director Proyectos	N. Teléfono	17
Ventas / Proceso1	Director Ventas	N. Teléfono	6
Administración / Proceso1	Director Administración	N. Teléfono	4
Infraestructura / Proceso1	Director Infraestructura	N. Teléfono	2
RR.HH. / Proceso1	Director RR.HH.	N. Teléfono	4
TOTALES			**123**

Tabla 1 – Tabla de criticidad de procesos

Una vez establecidos junto con cada Departamento los procesos críticos y su recuperación, se analizará la infraestructura de la Compañía, realizándose un inventario de todo el material que se considere imprescindible para el desarrollo de los procesos críticos de la Empresa. Este inventario es importante ya que existiría un listado en el que poder basar la recuperación en caso de que la integridad de dichos activos críticos para la Compañía se viera afectada por un desastre.

En la simulación realizada, se ha acordado con cada Departamento la inclusión del inventario detallado del mismo en cada Plan de Recuperación Departamental. Se detalla en la siguiente tabla el inventario del Departamento de Sistemas y Seguridad, por afectar a todos los Departamentos, ser básico para la elaboración del DRP y estar directamente relacionado en la elaboración del BCP.

ELEMENTO	MODELO	CANTIDAD	UBICACION
Teléfono Fijo	Cisco IP Phone 6940	160	Oficina
Teléfono Fijo	Cisco IP Phone 6940	12	Stock
Teléfono Móvil	Samsung Galaxy Core	8	Dirección
Teléfono Móvil	Samsung Galaxy Mini	10	Operaciones
Teléfono Móvil	Samsung Galaxy Mini	5	Ventas
Teléfono Móvil	Samsung Galaxy Mini	4	Proyectos
Monitor	Monitor HP 21”	155	Oficina
Monitor	Monitor HP 24”	8	Dirección
Portátil	HP Elitebook 8470p	8	Dirección
Portátil	HP Probook 6460b	87	Operaciones
Portátil	HP Probook 6470b	54	Proyectos
Portátil	HP Probook 6470b	1	Sistemas
Portátil	HP Probook 6470b	5	Ventas
Portátil	HP Probook 6470b	10	Stock
Ordenador	HP Compaq 8000 Elite SFF	3	Administración
Ordenador	HP Compaq 8000 Elite SFF	1	Infraestructura
Ordenador	HP Compaq 8000 Elite SFF	3	RR.HH.
Impresora	Canon IR 2020 Color	2	Operaciones
Impresora	Canon IR 2020 Color	1	Proyectos
Impresora	Canon IR 2020 Color	1	Ventas
Impresora	HP Laserjet 4300	2	Administración
Impresora	HP Laserjet 4300	1	RR.HH.
Modem USB 4G	Modem USB 4G	8	Sistemas
Alarma	Alarma de seguridad	1	Sistemas
Cámaras seguridad	Samsung SND-6011R	4	Sistemas

Control de acceso	Lectores control acceso	3	Sistemas
Videograbador	Samsung SHR-2162N	1	Sistemas
Servidores DHCP/DNS	HP Proliant ML110G5	1	Sistemas
Servidores Apps	HP Proliant DL120	2	Sistemas
Servidor Datos	HP Proliant X 1600	1	Sistemas
Backup syst.	HP StorageWorks Utrium 1760	1	Sistemas
UPS	Smart UPS RT-5000	2	Sistemas
RACKS	APC AR-3100	2	Sistemas
Firewalls	CISCO ASA 5520	2	Sistemas
Switches	CISCO Catalyst 3750G 48 puertos	6	Sistemas
Comms	CISCO 2811 Jazztel	1	Sistemas
Wifi	Linksys CISCO WRT 160	2	Sistemas
HDD USB Backups	Seagate 1 TB	3	Sistemas
Cintas backups	Cintas HP LTO4 Utrium 1.6TB	20	Sistemas

Tabla 2 – Inventario Sistemas Y Seguridad

Una vez obtenido el inventario físico, indicando la ubicación por departamento para facilitar la recuperación si fuera necesario, se analizará la configuración de las conexiones de la Compañía. El conocimiento de la estructura de las conexiones nos permitirá tanto disponer de un análisis detallado de la situación actual, como fijar el objetivo final en un eventual proceso de recuperación, sin olvidar ningún aspecto al disponer de una imagen de la situación inicial.

En la simulación que nos ocupa, se ha obtenido el diagrama siguiente representando la configuración actual de las conexiones de SPBCP Consulting, tras ser analizado por el Departamento de Sistemas y Seguridad:

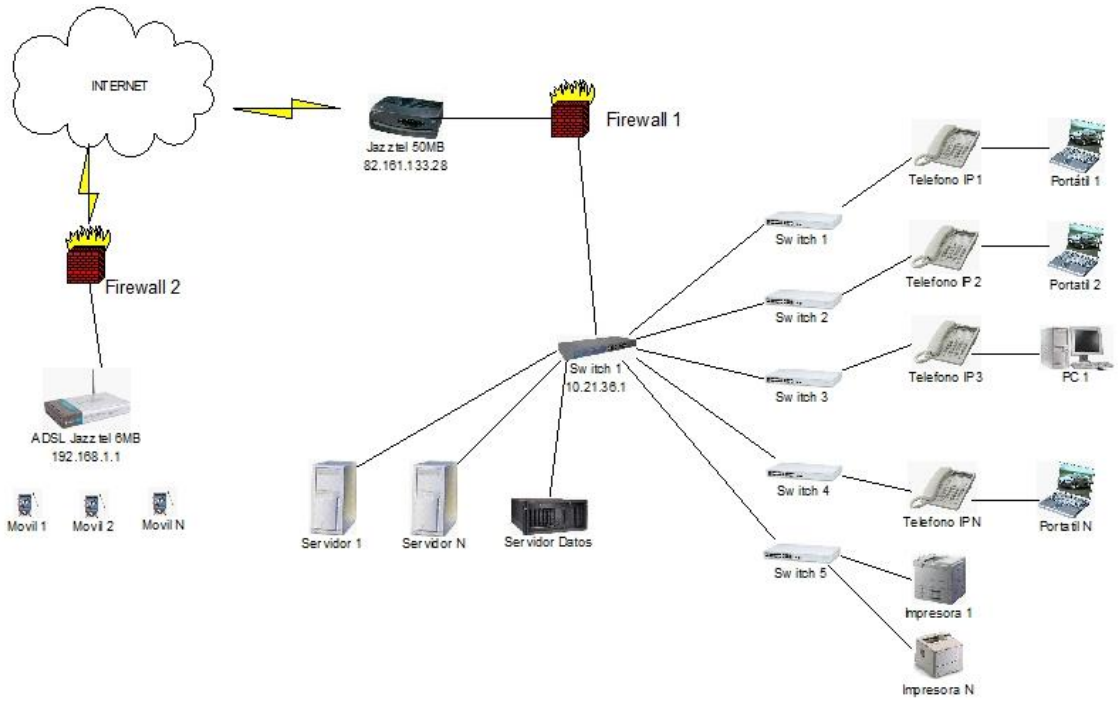


Figura 3 – Esquema de conexiones de red

A continuación se analizarán las medidas de seguridad con las que cuenta la Compañía para poder mitigar los daños en caso de desastre. Estas medidas pueden ser tanto lógicas como físicas, y tanto preventivas como reactivas. Es importante el análisis de las medidas de seguridad actuales, ya que nos dará la oportunidad de revisarlas, mejorarlas o actualizarlas e implantar unas nuevas medidas de seguridad estandarizadas y adecuadas a la situación actual mediante la implantación del BCP.

En la simulación que estamos llevando a cabo, se ha efectuado una reunión de 2 horas con los responsables de los Departamentos de Generales y de RR.HH., donde se han puesto en común los sistemas, medidas y políticas de seguridad con los que cuenta la Compañía. Estas medidas se resumen en la siguiente tabla.

ELEMENTO	DESCRIPCIÓN	RESPONSABLE
Detectores Humo	10 detectores de humo	Infraestruct.
Extintores	10 extintores	Infraestruct.
Sistema eléctrico	Protecciones y fases diferenciadas	Infraestruct.
Botiquín	Primeros auxilios	RR.HH.
Vigilante de seguridad	Vigilante 24x7	Edificio

Alarma	5 detectores movimiento + centralita	Sistemas
Cámaras de seguridad	4 cámaras + grabador	Sistemas
Control de acceso electrónico	4 lectores acceso + software	Sistemas
Acceso usuarios a sistemas	Acceso protegido por contraseña	Sistemas
Seguridad equipos	Antivirus corporativo	Sistemas
Seguridad servidores	Acceso restringido Sistemas	Sistemas
Seguridad de red	Firewalls	Sistemas
Copia seguridad servidores aps.	Semestral Cinta de almacenamiento	Sistemas
Copia seguridad servidor datos	Semanal Cinta de almacenamiento	Sistemas
Sistema UPS racks	2 UPS / 30 minutos	Sistemas
Políticas de seguridad informática para empleados	Políticas por escrito firmadas por todos los empleados	RR.HH.
Seguros	Cobertura empleados y material	RR.HH.

Tabla 3. Medidas iniciales de seguridad

Por último también es importante analizar las instalaciones en las que se ubica la Empresa. Mediante este análisis se obtendrá una valiosa información acerca de los riesgos que pueden amenazar a la Compañía, posibles medidas de seguridad, tanto correctoras como preventivas implantadas en el edificio, contactos útiles, etcétera. Hay que tener en cuenta que, en caso de producirse un desastre que afecte a las instalaciones de la Compañía, el propietario de estas instalaciones podría convertirse en una parte importante del proceso de recuperación. Conviene, por tanto, tener en cuenta este aspecto en el análisis de la Compañía.

En la simulación que estamos tratando, la oficina se ubica en una de las plantas de un edificio de oficinas de Madrid. Este edificio es compartido por otras Empresas, ubicadas en otras plantas diferentes. Se ha mantenido una reunión con el propietario de la finca, consultándole sobre los posibles riesgos que podrían afectar a las instalaciones de SPBCP Consulting, las medidas de seguridad implantadas en el edificio, así como si disponen de algún plan de continuidad propio.

Como resultado de esta reunión, se ha obtenido la información de que la Compañía no está ubicada en un emplazamiento con alto riesgo de inundaciones, terremotos, huracanes, etc. Se ha comprobado que la Propiedad dispone de seguros en vigor que también cubren una parte de las propias instalaciones de SPBCP, y que también cuenta con diversas medidas de seguridad propias, tales como sistema anti-incendios, acceso restringido, sistema de alarma, vigilante de seguridad, cámaras de seguridad, etcétera . Por otra parte, la Propiedad también dispone de su propio Plan de Recuperación.

Figura 4 – Sede SPBCP Consulting S.A.

Una vez realizado el análisis preliminar de la Compañía ya se dispone de una situación base sobre la que empezar a construir el Plan de Continuidad.

En el ejemplo simulado, tras este análisis inicial conocemos mejor la situación actual de la Empresa, y podemos empezar a diseñar el nuevo Plan de Continuidad. Además, hemos logrado el apoyo de toda la Dirección de la Compañía, y se ha establecido formalmente un Equipo de Gestión de Continuidad.

Para realizar este análisis inicial la Dirección de Sistemas y Seguridad ha empleado 15 días laborables, y el gasto de esta fase ha sido de 0 €.

3.4.- Simulación del Análisis de Riesgos

En esta fase se deberán identificar, enumerar y evaluar los distintos riesgos y vulnerabilidades que pueden afectar a la Compañía, y ordenarlos de acuerdo a su probabilidad de ocurrencia e impacto en el desarrollo normal de las funciones del negocio.

En el ejemplo simulado, se han analizado los posibles riesgos a los que se puede enfrentar la Compañía a partir de la documentación anterior, de las experiencias obtenidas tras las reuniones con el Equipo de Gestión de Continuidad y de la información provista por la propiedad del edificio, en base a su experiencia.
Los grupos de riesgos resultantes tras la valoración de toda la información anterior han sido los siguientes:

- Riesgos Naturales.
- Riesgos Tecnológicos.
- Riesgos causados por errores no intencionados.
- Riesgos causados por acciones deliberadas.

Dichos riesgos ordenados por su clasificación se recogen en la siguiente tabla, indicando para cada uno de ellos la probabilidad de ocurrencia y el perjuicio que podría tener para el Negocio en caso de producirse, apareciendo también en dicha tabla el activo mayoritariamente afectado.

RIESGO	TIPO DE RIESGO	PROBABILIDAD	PERJUICIO	AFECTACION
Fuego	Natural	BAJA	ALTO	Infraestructura / Datos
Inundaciones	Natural	BAJA	ALTO	Infraestructura / Datos
Terremotos	Natural	BAJA	ALTO	Infraestructura
Meteorología adversa	Natural	MEDIA	BAJO	Infraestructura
Epidemias / Plagas	Natural	MEDIA	MEDIO	Personal
Fallo suministro eléctrico	Tecnológico	MEDIA	MEDIO	Infraestructura / Datos
Fallo comunicaciones	Tecnológico	MEDIA	BAJO	Datos
Fallo refrigeración	Tecnológico	BAJO	MEDIO	Sistemas
Fallo hardware	Tecnológico	MEDIA	BAJO	Sistemas
Fallo software	Tecnológico	MEDIA	BAJO	Datos
Errores usuarios	Errores NI	MEDIA	MEDIO	Datos
Errores administrador	Errores NI	BAJA	ALTO	Datos
Errores mantenimiento	Errores NI	BAJA	MEDIO	Sistemas

Errores configuración	Errores NI	BAJA	BAJO	Sistemas
Virus informático	Deliberado	ALTA	MEDIO	Sistemas / Datos
Hackers	Deliberado	MEDIA	ALTO	Sistemas / Datos
Suplantación identidad	Deliberado	BAJA	ALTO	Datos
Fraude	Deliberado	BAJA	ALTO	Datos
Robo información	Deliberado	BAJA	ALTO	Datos
Vandalismo / Robo	Deliberado	BAJA	ALTO	Infraestructura
Terrorismo	Deliberado	BAJA	ALTO	Infraestructura

Tabla 4 – Análisis de Riesgos

Para realizar el análisis de riesgos la Dirección de Sistemas y Seguridad ha empleado dos días laborables, y el gasto de esta fase ha sido de 0 €.

3.5.- Simulación del Análisis de Impacto al Negocio

A continuación elaborará el Análisis de Impacto al Negocio. Este análisis nos proporcionará información sobre los procesos críticos de la Empresa, su tiempo máximo de inactividad y la valoración del impacto al negocio en cada momento. Es de suma importancia para el BCP, ya que establece la pauta y prioridad de recuperación de los diferentes procesos críticos de la Compañía.

En la simulación que estamos realizando, se han realizado reuniones de 1.5 horas de duración con cada Director de Departamento, para analizar los procesos críticos de la Compañía desde el punto de vista de cada área. En estas reuniones también se ha actualizado la situación del Plan de Recuperación Departamental de cada área, estando muy avanzada su elaboración en todos los Departamentos.

Para la elaboración del Análisis de Impacto al Negocio se tendrán en cuenta los siguientes parámetros para cada proceso crítico, de acuerdo con la información proporcionada por el Director de cada área:

- Nombre del Proceso y Departamento al que pertenece.
- Tiempo Máximo de Interrupción (T.M.I.) para cada proceso.
- Tiempo de Recuperación Objetivo (T.R.O.) para cada proceso. Es el tiempo necesario esperado para la recuperación de un proceso crítico de la Empresa en caso de que este proceso haya sufrido una interrupción.
- Personal mínimo necesario para la ejecución de cada proceso.

En la siguiente tabla se han recogido toda la información descrita anteriormente sobre los procesos críticos para la Compañía, después de realizar el Análisis de Impacto al

Negocio en conjunto con todas las áreas de la Empresa. El orden de aparición en la tabla establece también el orden de prioridad en caso de ser necesaria la recuperación.

DEPT. / PROCESO	T.M.I.	T.R.O.	PERSONAL
Sistemas / Comunicaciones + Datos	36 horas	24 horas	1
Operaciones / Proceso1	36 horas	24 horas	8
Operaciones / Proceso2	36 horas	24 horas	8
Operaciones / Proceso3	48 horas	24 horas	6
Proyectos / Proceso1	36 horas	24 horas	8
Proyectos / Proceso2	36 horas	24 horas	6
Ventas / Proceso1	48 horas	24 horas	1
Administración / Proceso1	36 horas	24 horas	2
Infraestructura / Proceso1	48 horas	24 horas	1
RR.HH. / Proceso1	48 horas	24 horas	2
TOTALES			**43**

Tabla 5 – Análisis de Impacto al Negocio

Una vez analizados los procesos críticos de la Compañía y habiéndolos registrado en la tabla anterior, se ha realizado una nueva reunión de una hora entre todo el Equipo de Gestión de Continuidad para analizar estos datos y confirmar con la Dirección que se trata de estimaciones realistas, así como para proveer una actualización de la situación de la implantación del Proyecto. Una vez aprobados estos datos por todos los equipos queda establecido el Análisis de Impacto al Negocio.

Para realizar el análisis de riesgos la Dirección de Sistemas y Seguridad ha empleado cuatro días laborables, y el gasto de esta fase ha sido de 0 €.

3.6.- Simulación de Estrategia del BCP

Una vez que se tiene un conocimiento profundo de la Compañía y sus procesos, se han detectado los riesgos y amenazas a los que ésta se puede enfrentar, y se ha determinado el impacto que tendría para la Empresa la interrupción de sus procesos críticos, se puede establecer una estrategia para el Plan de Continuidad.

Esta estrategia tratará de diseñar e implantar las medidas necesarias, tanto de prevención como de recuperación, para minimizar en lo posible el impacto de todas las amenazas que puede afrontar la Empresa en caso de que estas llegaran a producirse.

En el caso simulado, la Dirección de Sistemas y Seguridad, junto con los responsables de otras áreas, realizará un listado de las medidas preventivas implantadas en SPBCP Consulting S.A. en el momento del análisis, y propondrá las medidas adicionales necesarias para dotar a la Empresa de unas medidas preventivas acordes a su situación.

Por otra parte también se estudiarán y especificarán los procesos de recuperación en vigor, de forma que puedan ser analizados, mejorados y recogidos en el Plan de Continuidad para ser aplicados en caso necesario.

Se ha realizado por parte de la Dirección de Sistemas, con apoyo del resto de Departamentos, varias reuniones para establecer la situación actual e implementar las mejoras oportunas. Posteriormente en una reunión de 1 hora con el Equipo de Gestión de Continuidad se ha validado el resultado y obtenido la siguiente tabla de medidas preventivas, donde se detallan las medidas, la situación actual, la situación deseada y el coste de implantación de cada medida, en caso de que deba ser actualizada. Si se trata de contratos de mantenimiento en vigor con un coste periódico éste no se ha contemplado en la tabla, ya que no supone ninguna diferencia con la situación actual y es un gasto ya presupuestado que no forma parte del proyecto de implantación.

MEDIDA PREVENTIVA	SITUACIÓN ACTUAL	SITUACIÓN DESEADA	COSTE €
Sistemas Antiincendios	Revisiones semestrales	Sin cambios	0 €
Instalaciones Eléctricas	Revisiones anuales	Sin cambios	0 €
Alarma	Revisiones semestrales	Sin Cambios	0 €
Cámaras de Seguridad	Revisiones anuales	Sin Cambios	0 €
Inventario actualizado	En vigor	Sin Cambios	0 €
Conexiones redundantes	No	Añadir conexión de datos redundante	2875 € / anuales
Alimentación Ininterrumpida	2 UPS	2 UPS + pack de baterías	2.750 €
Aires Acondicionados	2 unidades. Revisión semestral	3 unidades. Revisión semestral.	1.250 €
Copias de seguridad	Datos -> Semanales Software -> Semestrales Almacenamiento interno	Datos -> Diarias Software -> Mensuales Almacenamiento externo	2890 € anuales
Sistemas Operativos	Windows 7 Windows Server 2008	Sin cambios	0 €
Antivirus	Panda Endpoint Antivirus Actualizado	Ampliar a los 27 teléfonos móviles	1891 € anuales
Firewalls	2 FW actualizados	Sin cambios	0 €
VPN	No existe	Implantar VPN	0 €
Equipos informáticos	No obsoletos Existencia 7 equipos sobremesa	Reemplazar equipos sobremesa por portátiles	4250 €
Módems móviles USB 4G	8 módems para Dirección	Uso de datos móviles como módems en los 27	4860 € anuales

		dispositivos	
Control de acceso edificio	Control electrónico	Sin cambios	0 €
Políticas de seguridad	Revisiones anuales	Sin cambios	0 €
Formación seguridad empleados	A la contratación	Formaciones anuales	3500 € anuales
Sistemas antirrobo portátiles	No existente	Adquisición de candados	3820 €

Tabla 6. – Medidas de seguridad preventivas y acciones a tomar

Una vez revisadas las medidas de preventivas actuales de mitigación de riesgos, se ha concluido que sería necesaria una inversión para el año en curso de 28.086 € tras realizar las modificaciones indicadas en la tabla. Se han necesitado 11 jornadas de trabajo del Director de Sistemas para realizar este análisis.

La implantación de estas mejoras dotará a la Compañía de ciertas medidas preventivas que mitigarán los riesgos antes, durante o después de que sucedan, mejorando las instalaciones, los dispositivos o facilitando el trabajo desde otras localizaciones que no sean la principal. Sin embargo, si el desastre finalmente se produce, será necesario contar con estrategias de recuperación adecuadas que poder llevar a cabo para ser capaces de restaurar la situación inicial en el menor tiempo posible.

Respecto a estas estrategias de recuperación, se han realizado reuniones con todos los departamentos para elaborar cuáles serían las acciones necesarias en caso de que se produjera un desastre. Posteriormente a estas reuniones con cada Departamento, se ha puesto toda la información en una reunión adicional de 2 horas con todo el Equipo de Gestión de Continuidad, habiendo validado la Dirección General las estrategias mencionadas. Dicha información se ha recogido en la tabla a continuación, estando representada la prioridad en la ejecución de las estrategias en el orden en la tabla:

ESTRATEGIA	DETALLE
Estrategia Líder / RR.HH.	Evaluación situación Convocatoria Equipo Gestión Continuidad Organización Empleados Aplicación PRD Comunicaciones Internas Comunicaciones Externas
Estrategia Infraestructura	Evaluación daños Localización alternativa Aplicación PRD Contacto proveedores
Estrategia Sistemas	Evaluación daños Aplicación DRP Sistemas

	Recuperar comunicaciones Recuperar sistemas Recuperar datos Recuperar seguridad
Estrategia Operaciones	Aplicación PRD
Estrategia Proyectos	Aplicación PRD
Estrategia Administración	Disposición fondos contingencia para recuperación Cuantificación daños Contacto seguros / legal Aplicación PRD
Estrategia Ventas	Contacto clientes Aplicación PRD

Tabla 7. – Estrategia Recuperación BCP

Para la realización de esta Estrategia la Dirección de Sistemas ha necesitado 8 días laborables, con un coste total de 0 € para esta fase.

3.7.- Simulación de Desarrollo del BCP

Una vez que se ha establecido la estrategia de recuperación del BCP se puede detallar el desarrollo de dicha estrategia, estableciendo un Plan de Crisis y los pasos necesarios detallados que se llevarían a cabo si fuese necesaria la ejecución del Plan de Contingencia.

En el caso de SPBCP Consulting, la Dirección de Sistemas ha realizado reuniones de 1 hora con cada Director de área para concretar los pasos que se llevarían a cabo de manera ordenada, y recabar los datos necesarios para la elaboración de esta parte de la documentación final del BCP (datos de contactos de clientes, proveedores, etc.).
Tras la unificar todos los datos se ha realizado una nueva reunión de todo el Equipo de Gestión, de 1 hora de duración, donde se ha consolidado la información y aprobado el desarrollo del plan de continuidad por parte de todo el Equipo de Gestión.

La tabla a continuación recoge en detalle los pasos necesarios para el desarrollo del Plan de Continuidad.

ACCIÓN	RESPONSABLE
La persona que decide la ejecución del BCP debe disponer de toda la información posible: - Localización y momento del incidente. - Si existen heridos o víctimas mortales. - Alcance y gravedad de los daños. - Impacto de primer nivel: edificio no accesible, corte eléctrico… - Convocar al Equipo de Gestión de Continuidad.	Líder Equipo Gestión Continuidad
Acciones una vez convocado el Equipo de Gestión de Continuidad: - Si la Oficina no está disponible, cuantificar el posible tiempo de no disponibilidad y buscar lugar de trabajo alternativo para el personal crítico. - Establecer un lugar y fecha para la primera reunión del Equipo. - Informar al resto de empleados para que, cuando sea posible, puedan teletrabajar desde sus domicilios. - Gestión por parte de RR.HH. de la posible existencia de heridos o víctimas mortales.	Equipo de Gestión de Continuidad
Primeras 24 horas: Equipo de Gestión de Continuidad: - Actualizar la información de todos los Departamentos. - Asegurar que las instalaciones de la empresa son seguras y que no se permite el acceso a ninguna persona excepto a las Autoridades Locales o el Equipo de Gestión de Continuidad. - Establecer la mejor forma de comunicación en base a la infraestructura existente. - Organizar estancia en hoteles, caterings, etc.para el Equipo de Gestión de Continuidad. - Establecer reuniones periódicas de actualización.	Equipo de Gestión de Continuidad
Primeras 48 horas: Equipo de Gestión de Continuidad: - Identificar los daños a los activos de la Empresa - Determinar el tiempo de inoperatividad - Determinar si es necesario realizar desvíos telefónicos - Comunicaciónes internas a los empleados - Considerar la necesidad de comunicaciones externas - Si es necesario, buscar ubicación alternativa para lanzar el Plan de Recuperación, dependiendo del tiempo estimado de no disponibilidad de las infraestructuras.	Equipo de Gestión de Continuidad
Primeras 48 horas: Departamento de Infraestructura - Evaluación daños - Búsqueda de lugares alternativos si fuera necesario	Infraestructura
Primeras 48 horas: Departamento de Sistemas y Seguridad:	Sistemas

- Evaluación de los daños - Recuperación Comunicaciones - Recuperación Sistemas - Recuperación Datos	
Primeras 48 horas: Departamento de Operaciones: - Teletrabajo personal crítico	Operaciones
Primeras 48 horas: Departamento de Proyectos: - Teletrabajo personal crítico	Proyectos
Primeras 48 horas: Departamento de Administración: - Disponibilidad fondos recuperación - Cuantificación económica de daños - Contacto con los seguros - Contacto con proveedores críticos	Administración
Primeras 48 horas: Departamento de Ventas: - Contacto con clientes críticos	Ventas
Primeras 48 horas: Departamento de RR.HH. - Atención a los Empleados - Soporte a las distintas áreas de la Compañía para cubrir las necesidades de recursos humanos.	RR.HH.
Días siguientes: - Reuniones periódicas del Equipo de Gestión - Ejecución de los distintos PRD de cada Departamento - Monitorización del proceso de Recuperación - Objetivo: Restaurar la actividad normal de la Compañía	Equipo de Gestión de Continuidad

Tabla 8. – Desarrollo del Plan de Continuidad

Para la realización de esta Estrategia la Dirección de Sistemas ha necesitado 10 días laborables, con un coste de 0 €.

3.8.- Simulación de Documentación del BCP

Como resultado de la elaboración del BCP se obtendrán diversos documentos que recojan toda la información y los procedimientos analizados y establecidos en las distintas fases del Plan de Continuidad. Esta documentación es de gran importancia, ya que servirá como guía en caso de ser necesaria la aplicación del mismo.

A continuación se indican los documentos obtenidos en el ejemplo simulado. Estos documentos serán propiedad de SPBCP Consulting S.A. y se mantendrán como Confidenciales. Todos los miembros del Equipo de Gestión de Continuidad deberán disponer de una copia actualizada del BCP.

A continuación se indican los documentos obtenidos tras la realización del Plan de Continuidad de Negocio:

- BIA (Business Impact Analysis): Este documento recoge el análisis de los posibles riesgos que pueden afectar a los sistemas y procesos de la Compañía, e incluye tanto el Análisis de Riesgos como el Análisis de Impacto. Este documento se puede encontrar en el Anexo I.

- Plan de Crisis: Este documento contiene la información necesaria para la gestión de la crisis desde los momentos iniciales, indicando aspectos tales como el personal a cargo de la recuperación, los contactos necesarios para la gestión de incidencias, los tiempos de resolución de incidencias, etc. Se ha diseñado indicando los pasos a seguir desde los primeros instantes de la ocurrencia del desastre, para disponer de una guía estandarizada de pasos que pueda ser de utilidad en una situación de posible desconcierto y nerviosismo. Este documento se detalla en el Anexo II.

- DRP (Disaster Recovery Plan): En este documento se han detallado los procesos necesarios para proteger y recuperar la infraestructura IT de SPBCP Consulting en caso de desastre. Contiene planes y políticas detalladas tanto de seguridad preventiva como las acciones planeadas para ejecutar una posible recuperación de los Sistemas. Este documento se detalla en el Anexo III.

- Plan de mantenimiento y pruebas: En este documento se recogen las políticas de mantenimiento del BCP en la Compañía, incluyendo las pruebas, revisiones y ejercicios prácticos necesarios para asegurar la consistencia del BCP con la situación de la Empresa en cada momento.

- BCP (Business Continuity Plan): El BCP propiamente dicho es el documento final que servirá de guía para la mitigación de posibles riesgos y la recuperación de la operatividad de la Compañía en caso de desastre. Se debe proporcionar una copia actualizada del mismo a cada miembro del Equipo de Gestión de Continuidad. Este documento se detalla en el Anexo IV.

- Documentación de formación a empleados: Adicionalmente a todos estos documentos, se ha elaborado una pequeña guía resumiendo los aspectos más importantes que deben tener en cuenta todos los empleados en referencia a la Continuidad de la Empresa. Esta documentación explica por qué es importante la continuidad, y detalla las medidas preventivas que todos los empleados deben adoptar para minimizar los riesgos que afronta la Empresa. Para su comunicación a todos los empleados se ha elegido la distribución mediante correo electrónico corporativo de un e-mail introduciendo el tema, y el documento adjunto a dicho mail, incluyendo las medidas preventivas de seguridad a tener en cuenta por todos los empleados. Asimismo se impartirá también formación sobre la materia de una hora a todos los nuevos empleados. Esta formación será responsabilidad del Departamento de RR.HH.

Para la elaboración de esta documentación han sido necesarias 25 jornadas laborables del Director de Sistemas, habiendo tenido un coste de 256 € en concepto de copias y papel.

3.9.- Simulación de Pruebas y Ensayos del BCP

Una vez finalizada la elaboración del Plan se reunirá por completo el Equipo de Gestión de Continuidad para revisar y validar todo el Plan completo. Una vez comprobada la posible validez teórica del mismo, se plantearán varios ensayos que sirvan como ejercicio que pueda simular una posible situación de necesidad de ejecución del BCP.
En SPBCP Consulting S.A. el Equipo de Gestión de Continuidad ha validado el BCP, y ha propuesto las pruebas y ensayos recogidas en el Anexo IV.

3.10.- Simulación de Mantenimiento del BCP

Una vez comprobada la validez del Plan habiéndose realizado las pruebas y ensayos indicadas en el apartado anterior, debe definirse una política de Mantenimiento del BCP que permita tener el mismo actualizado a pesar de los cambios que pudieran producirse en la Compañía.

En SPBCP Consulting S.A. se han establecido las siguientes políticas de mantenimiento para el BCP:

- Revisiones periódicas anuales de todo el proceso, promovidas por el Líder del Equipo de Gestión de Continuidad.

- Realización de un ejercicio anual, simulando una situación de crisis que provoque la ejecución simulada del Plan, y en el que esté presente todo el Equipo de Gestión de la Continuidad.

- Los Departamentos notificarán al Equipo de Gestión de Continuidad de cualquier cambio que pudiera suponer una modificación de la información contenida en el Plan, para estudiar si fuera necesaria la actualización del BCP.

- Si el Plan de Continuidad llegara a ejecutarse en algún momento, una vez que la situación vuelva a la normalidad el Equipo de Gestión de la Continuidad se reunirá para comprobar el funcionamiento del Plan después de su invocación y si fuera necesario algún cambio o actualización del mismo.

4.- PLANIFICACIÓN Y PRESUPUESTO

Para la elaboración de la planificación y el presupuesto del proyecto se han considerado 2 opciones: bien realizar el estudio para el Proyecto Fin de Carrera propiamente dicho, de la misma forma que se hace en otros Proyectos Fin de Carrera, o bien realizar el estudio para el proyecto de implantación de Business Continuity Plan expuesto en el Capítulo 3.

Finalmente, y con la ayuda del Tutor, se ha considerado que podría ser de más interés, dado el enfoque práctico de este PFC, realizar el estudio sobre la planificación del propio proyecto de implantación de BCP en la empresa simulada, SPBCP Consulting, con el objeto de proporcionar al lector un ejemplo de planificación que pueda servir de guía en una situación similar.

Una vez detallada la planificación del proyecto se elaborará un presupuesto para llevar a cabo la mencionada implantación. Este presupuesto incluirá tanto los costes del material necesario como del personal encargado del desarrollo de la implantación.

Así pues, en este apartado se va a detallar la planificación del proyecto de implantación del Business Continuity Plan que se realiza en la empresa ficticia SPBCP Consulting, desde la perspectiva del encargado de llevar a cabo el proyecto de implantación, esto es, el Director de Sistemas y Seguridad de dicha compañía ficticia.

4.1.- Planificación del Proyecto

Las necesidades del mundo empresarial de hoy en día obligan a implementar en las compañías medidas de seguridad y prevención que incrementen la confianza de los clientes y los accionistas en la empresa. No disponer de un Plan de Continuidad del negocio puede proporcionar una disminución de esta confianza, con la consiguiente imagen de pérdida de contratos, no adjudicación de nuevos contratos y, por tanto, pérdida del valor del negocio de la compañía. Es habitual, por tanto, que sea la Dirección de la compañía la que proponga y promueva la implantación de medidas de seguridad y prevención adecuadas para mantener el buen funcionamiento de la empresa.

De la misma manera, en la simulación la idea inicial del proyecto de implantación del BCP en SPBPC Consulting S.A. surge por parte de la Dirección de la compañía, que encarga la elaboración y mantenimiento del mismo al Departamento de Sistemas y Seguridad. Al estar formado por 2 personas, será el Director de este departamento el que tome la responsabilidad de la implantación y mantenimiento del Plan.

La planificación por parte del Director de Sistemas para la implantación del Plan de Continuidad ha constado en la división del proyecto en distintas fases, comenzando por el análisis de la compañía, para simplificar la tarea global y no olvidar ningún aspecto en el desarrollo del Plan.

El Director de Sistemas Y Seguridad ha dividido el proyecto de implantación en las fases a continuación:

- Análisis de la Compañía: En esta fase el responsable del proyecto (Director de Sistemas y Seguridad) se ha reunido con los responsables de los distintos departamentos que componen la empresa, así como con la Dirección General. De estas reuniones se ha obtenido una imagen de la situación de la compañía en el momento previo a la implantación del Plan, así como un Equipo de Gestión de la Continuidad, que será el encargado de dirigir y organizar el desarrollo del plan de continuidad si fuera necesaria su ejecución.

  Para la consecución de esta fase el Director de Sistemas Y Seguridad ha necesitado de 15 días laborables de trabajo a tiempo completo, contando con todas las reuniones, análisis, planificaciones y estudios necesarios para obtener y sintetizar toda la información.

- Análisis de Riesgos: Para la elaboración de esta fase el Director de Sistemas y Seguridad ha realizado, con la ayuda de las reuniones mantenidas durante la fase de análisis, de su experiencia y de documentación existente anteriormente, un estudio de los distintos riesgos y amenazas que afronta la compañía, tanto por las características de su negocio como por su localización y entorno. Este estudio será de gran importancia para la fase posterior, el análisis de impacto al negocio.

  Para esta fase han sido necesarias 2 jornadas completas de trabajo del Director de Sistemas y Seguridad, en las que ha recopilado y estudiado toda la información hasta obtener el análisis de riesgos.

- Análisis de Impacto al Negocio: A partir de la realización del análisis de riesgos en la fase anterior, y realizando nuevas reuniones con los responsables de cada departamento, se obtiene un estudio del posible impacto que pudiera sufrir en negocio si los procesos críticos de cada departamento se vieran interrumpidos durante una determinada cantidad de tiempo. Una vez establecido este impacto se coteja con el Equipo de Gestión de Continuidad al completo en una nueva reunión. En esta fase también se hace un seguimiento de la situación de cada Plan de Recuperación Departamental.

  Para la realización de esta fase se han necesitado 4 jornadas completas de trabajo del Director de Sistemas y Seguridad, entre reuniones, análisis de documentos, síntesis de la información, etcétera.

- Estrategia del BCP: En esta fase se ha diseñado la estrategia de continuidad de la Compañía, estableciendo las medidas preventivas y las estrategias de recuperación para paliar al máximo todos los posibles riesgos que pudiera afrontar el negocio. Para la consecución de esta fase se ha analizado la documentación anterior, se han realizado diversas reuniones con los responsables de cada Departamento, así como con el Equipo de Gestión de Continuidad, y finalmente esta Estrategia ha sido aprobada por todo el mencionado Equipo.

Con todas estas tareas, han sido necesarias 19 jornadas de trabajo del Director de Seguridad y Sistemas para desarrollar esta estrategia.

- Desarrollo del BCP: Esta fase describe los pasos necesarios a tomar por el Equipo de Gestión de Continuidad en caso de ser necesaria la ejecución del BCP. La definición de esta fase dará lugar al Plan de Crisis, que será de gran utilidad para el Equipo de Gestión en una situación de crisis como las que plantea el Plan de Continuidad.

  Para esta fase el Director de Sistemas y Seguridad ha necesitado de 10 días laborables a tiempo completo, con subtareas como reuniones con los responsables de cada Departamento, análisis de la información, planificación de la estrategia, puesta en común con el Equipo de Gestión de Continuidad, aprobación del desarrollo de la estrategia, etcétera.

- Documentación del BCP: Todo el trabajo realizado en las fases previas serviría de muy poco si no quedara debidamente documentado, para poder hacer uso del mismo en cualquier momento que fuera necesario. Como resultado de esta fase se obtendrán varios documentos finales que quedarán en propiedad de la Compañía, siendo tratados por la misma como documentos internos y confidenciales. Estos documentos son confeccionados por el Director de Sistemas y Seguridad como responsable del BCP, y comprenden los siguientes: BIA, Plan de Crisis, DRP, Mantenimiento y pruebas del BCP y Plan de Continuidad propiamente dicho.

  Para la elaboración de estos documentos el Director de Seguridad y Sistemas ha necesitado de 25 días laborables, donde se ha sintetizado toda la información recopilada en las fases anteriores, obteniendo los documentos finales del BCP. Asimismo se ha diseñado y elaborado un Plan de Mantenimiento y Pruebas que servirá para mantener el BCP actualizado y al Equipo de Gestión de Continuidad entrenado ante la posibilidad de que fuera necesaria la ejecución del Plan.

4.2.- Diagrama de Gantt

A partir de la planificación del proyecto explicada en el apartado anterior, se ha obtenido el Diagrama de Gantt a continuación. Este diagrama representa el camino de un proyecto basándose en el origen, el final y la precedencia de las distintas unidades mínimas de trabajo.

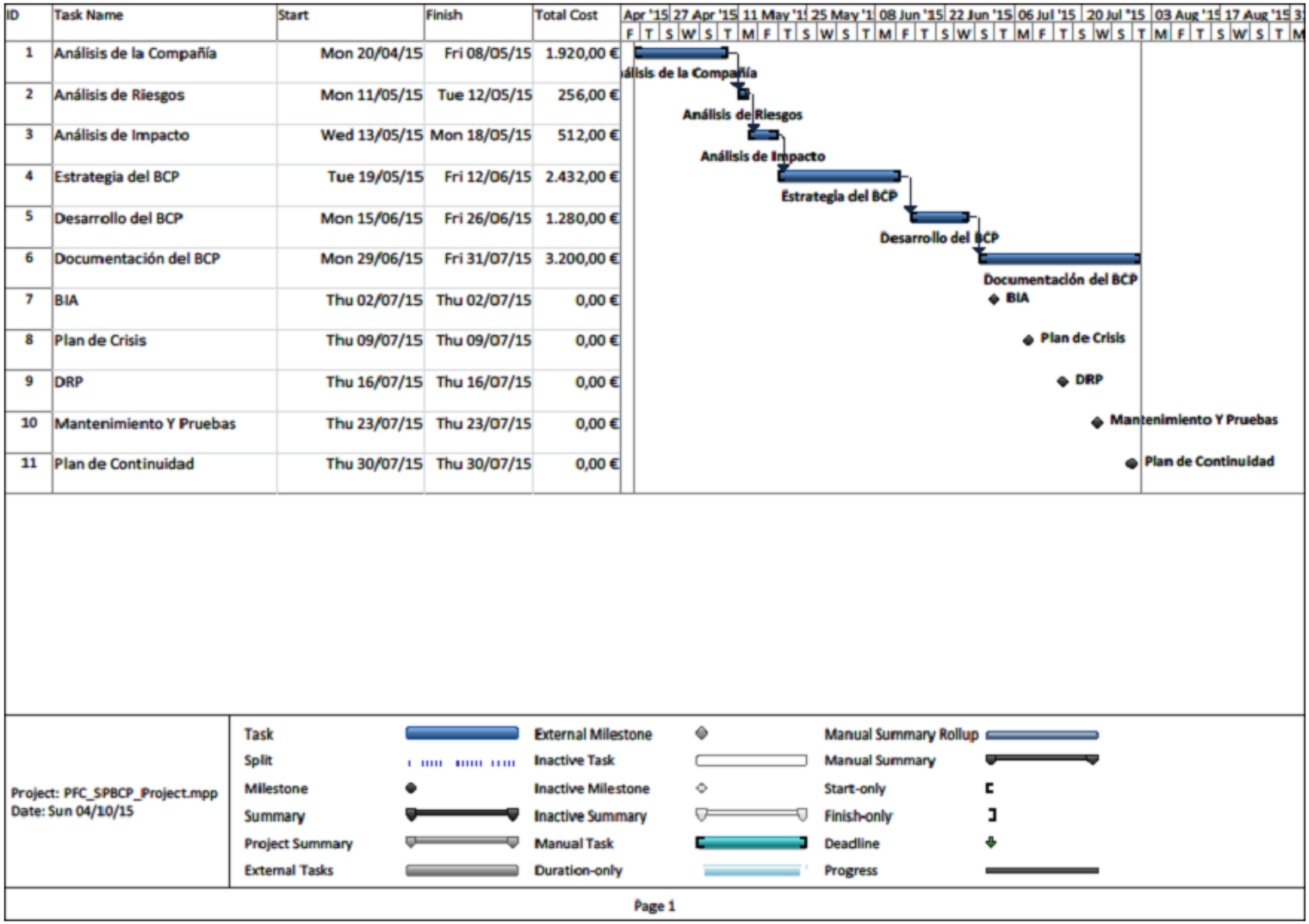
En este proyecto de implantación del Plan de Continuidad se han establecido como unidades mínimas de trabajo del proyecto cada una de las fases explicadas en el punto anterior. La fase siguiente no puede comenzar hasta la finalización de la fase precedente, tal como representan las flechas del diagrama.

Además, en dicho diagrama se han marcado como hitos (milestones en inglés) la finalización de cada uno de los documentos propios del Plan de Continuidad. Los propios documentos serían los hitos del proyecto, al ser el producto visible del mismo.

Este diagrama se ha elaborado con la herramienta MS Project. Dicha herramienta permite gran cantidad de funciones en relación a la gestión de Proyectos. Por ejemplo permite la asignación de recursos a tareas, e incluso, introducidos los datos necesarios en la aplicación, es capaz de obtener datos y estadísticas avanzados, tales como el coste de cada tarea a partir de los recursos necesarios para ejecutarlas.

En el ejemplo, se han asignado todas las tareas al Director de Seguridad y Sistemas, para el que se ha establecido un coste de 16 €/hora (que correspondería a 33.280 € de coste anual para la Empresa). A partir del coste de este recurso, Microsoft Project es capaz de calcular el coste de cada tarea, tal como se indica en la columna Total Cost de la figura que representa el Diagrama de Gantt.

En la página siguiente se muestra el Diagrama de Gantt correspondiente al proyecto de implantación del BCP en la compañía simulada SPBCP Consulting S.A.



ID	Task Name	Start	Finish	Total Cost
1	Análisis de la Compañía	Mon 20/04/15	Fri 08/05/15	1.920,00 €
2	Análisis de Riesgos	Mon 11/05/15	Tue 12/05/15	256,00 €
3	Análisis de Impacto	Wed 13/05/15	Mon 18/05/15	512,00 €
4	Estrategia del BCP	Tue 19/05/15	Fri 12/06/15	2.432,00 €
5	Desarrollo del BCP	Mon 15/06/15	Fri 26/06/15	1.280,00 €
6	Documentación del BCP	Mon 29/06/15	Fri 31/07/15	3.200,00 €
7	BIA	Thu 02/07/15	Thu 02/07/15	0,00 €
8	Plan de Crisis	Thu 09/07/15	Thu 09/07/15	0,00 €
9	DRP	Thu 16/07/15	Thu 16/07/15	0,00 €
10	Mantenimiento Y Pruebas	Thu 23/07/15	Thu 23/07/15	0,00 €
11	Plan de Continuidad	Thu 30/07/15	Thu 30/07/15	0,00 €

Figura 5 – Diagrama de Gantt

4.3.- Presupuesto del Proyecto

A continuación se especifican los costes del proyecto de implantación del BCP en SPBCP Consulting S.A., pudiendo encontrarse el presupuesto en la página siguiente.

Para calcular estos costes se han tenido en cuenta los siguientes aspectos:

- Costes de personal: Se ha calculado el coste de personal del proyecto a partir del coste por hora derivada del salario del Director de Sistemas Y Seguridad. Se ha considerado un salario de 33.280 € anuales para esta posición, que resultan en un coste de 16 euros / hora.

  El proyecto tiene una duración total en todas sus fases de 600 horas, con lo que el coste del proyecto imputable a costes de personal asciende a 600 * 16 = 9600 euros.

  Coste de personal: 9600 €

- Coste de material: En la fase de Estrategia del BCP se han propuesto determinadas medidas preventivas a implantar en la Compañía para disponer de una infraestructura que minimice los riesgos, de acuerdo al BCP. El coste de todas estas mejoras (detalladas en la tabla 6 – Medidas de seguridad preventivas y acciones a tomar) se ha valorado en 28086 €, y también deben ser incluidos en el presupuesto final del proyecto de implantación del BCP, si se quiere disponer de un Plan de Continuidad con unas medidas de seguridad preventivas adecuadas a la realidad empresarial actual.

  Coste de material: 28086 €

- Consumibles informáticos: Como resultado del Proyecto, se han obtenido varios documentos finales, de los que se realizarán varias copias. El coste de impresión y copia de estos documentos ha ascendido a 256 euros.

  Coste de consumibles informáticos: 256 €

- Los costes directos del proyecto se obtiene de la suma de todos los costes anteriores, y asciende a 37.942 €.

- Indicar que se ha tenido en cuenta el coste correspondiente al resto de integrantes del Equipo de Gestión de Continuidad como costes indirectos. Aunque la asignación de las tareas ha sido realizada principalmente por el Director de Sistemas Y Seguridad, los demás miembros del Equipo de Gestión también han llevado a cabo reuniones, han participado en proveer información de sus Departamentos y han realizado sus propios Planes de Recuperación departamentales. Se incluirán estos costes y todos los demás no previstos como parte de los costes indirectos (20% del total del proyecto): 7588 €

- El coste total asciende, por tanto, a 37.942 € + 7588 € = 45.530 €

UNIVERSIDAD CARLOS III DE MADRID
Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

1.- Autor:
Samuel Pascual Martín
2.- Departamento:
Departamento de Informática
3.- Descripción del Proyecto:

- Titulo	**Business Continuity Plan - Conceptos Teóricos Y Simulación Práctica**	
- Duración (meses)	**3,46**	
Tasa de costes Indirectos:		20%

4.- Presupuesto total del Proyecto (valores en Euros):

	Euros	45.530

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	N.I.F. (no rellenar - solo a titulo informativo)	Categoría	Dedicación (hombres mes) [a]	Coste hombre mes	Coste (Euro)	Firma de conformidad
Director Sistemas Y Seguridad		Jefe Proyecto	3,46	2.774,56	9.599,98	
					0,00	
					0,00	
					0,00	
					0,00	
		Hombres mes	**3,46**	**Total**	9.599,98	

[a] 1 Hombre mes = 131,25 horas. Máximo anual de dedicación de 12 hombres mes (1575 horas)
Máximo anual para PDI de la Universidad Carlos III de Madrid de 8,8 hombres mes (1.155 horas)

EQUIPOS

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable [d]
Mejora Conexiones	2.875,00	100	60	60	2.875,00
Mejora Equipamiento	8.250,00	100	60	60	8.250,00
Mejora Seguridad	8.601,00	100	60	60	8.601,00
Conexiones móviles	4.860,00	100	60	60	4.860,00
Formación a empleados	3.500,00	100	60	60	3.500,00
					0,00
				Total	28.086,00

[d] Fórmula de cálculo de la Amortización:

$$\frac{A}{B} x C x D$$

A = nº de meses desde la fecha de facturación en que el equipo es utilizado
B = periodo de depreciación (60 meses)
C = coste del equipo (sin IVA)
D = % del uso que se dedica al proyecto (habitualmente 100%)

SUBCONTRATACIÓN DE TAREAS

Descripción	Empresa	Coste imputable
	Total	0,00

OTROS COSTES DIRECTOS DEL PROYECTO[e]

Descripción	Empresa	Costes imputable
Copias documentos		256,00
	Total	256,00

[e] Este capítulo de gastos incluye todos los gastos no contemplados en los conceptos anteriores, por ejemplo: fungible, viajes y dietas,

6.- Resumen de costes

Presupuesto Costes Totales	**Presupuesto Costes Totales**
Personal	9.600
Amortización	28.086
Subcontratación de tareas	0
Costes de funcionamiento	256
Costes Indirectos	7.588
Total	45.530

Figura 6 – Presupuesto de Implantación

5.- Conclusiones

Después de decidir la temática de este PFC empecé a investigar sobre el mismo en diversos libros, páginas de internet, revistas, etc… con la idea de descubrir un poco más a fondo en qué consistía la continuidad de los negocios, así como los planes de continuidad de los que tan poco había oído hablar en anteriores ocasiones.

Poco a poco me fui dando cuenta de la importancia del tema, hasta el punto de que si me preguntaran ahora mismo diría que, en el mundo empresarial actual, disponer de un plan formalizado de este tipo es básico para cualquier compañía. Nunca se sabe cuándo puede suceder un desastre que afecte de forma crítica a cualquier negocio, y estar preparados para afrontarlo nunca está de más. Incluso al contrario, la falta de este plan podría conducir a que la Empresa perdiera contratos, prestigio y, por tanto, valor, al no disponer de algo que los clientes solicitan hoy en día a sus proveedores.

El disponer de un plan de este tipo dotará a la empresa, aparte del plan propiamente dicho, de varias medidas de seguridad tanto de recuperación como preventivas, con las que poder mitigar los riesgos que puedan afectar a la compañía. Simplemente el hecho de analizar las vulnerabilidades de la compañía y ver cómo se pueden mitigar en lo posible ya supone, a mi juicio, un trabajo realmente útil para cualquier negocio.

También considero muy positiva para cualquier empresa la posibilidad de disponer además de unas políticas de recuperación ante un desastre, y de un plan de crisis que pueda ir guiando paso a paso a la dirección de la compañía en la recuperación de la misma en un límite de tiempo en que el impacto sea mínimo. Estas herramientas, que son relativamente sencillas de implantar en una compañía, serán de una enorme utilidad en caso de desastre y evitarán grandes pérdidas de tiempo y dinero al tener previstas las posibles situaciones que pudieran darse.

Considero hasta aquí, por tanto, que se han cumplido los 2 primeros objetivos que se establecieron al inicio de este PFC: Mostrar la necesidad de las empresas de disponer de un Plan de Continuidad y explicar tanto en qué consiste el mismo como los diferentes conceptos teóricos asociados a él.

En cuanto al tercer objetivo, la idea me surgió habiendo decidido ya que trataría mi proyecto de fin de carrera sobre los plantes de continuidad. Respecto al mismo, pensé que sería de utilidad al lector no sólo estudiar en profundidad los planes de continuidad, sino ofrecer una aproximación práctica con una empresa simulada, sobre la que el lector pudiera observar paso a paso cómo elaborar un plan de continuidad desde su fase inicial. Es cierto que este proyecto se enfoca en una empresa ficticia del sector de la consultoría informática, pero las fases pueden ser extrapolables a cualquier compañía de cualquier tipo, ya que, en base, la idea es analizar la compañía, estudiar sus vulnerabilidades y proveer y documentar soluciones.

Para la consecución de este tercer objetivo considero también que es de gran ayuda el ofrecer unos ejemplos reales del aspecto que tendrían los documentos definitivos asociados al Plan de Continuidad de una compañía, ya que al observar el aspecto que tienen dichos documentos el lector puede hacerse una idea de cómo realizar el propio Plan de Continuidad de Negocio en el caso que le ocupe.

Teniendo todo lo anterior en cuenta, puedo decir en este momento que estoy muy satisfecho tanto de haber elegido este tema como de la consecución de los objetivos que se fijaron al inicio del Proyecto.

No obstante, este PFC deja abierta la posibilidad de poder seguir realizando trabajos futuros sobre el mismo. Teniendo en cuenta que las empresas son entes vivos, y que la tanto la tecnología como las amenazas van cambiando y evolucionando a lo largo de los años, tanto los riesgos como las soluciones propuestas pueden revisarse en el futuro, y podrían adecuarse las medidas de seguridad a los nuevos riesgos, o actualizarse las medidas existentes por evolución tecnológica.

Por tanto podría revisarse este trabajo dentro de unos años desde la nueva perspectiva que ofrezca la situación empresarial en ese momento, incluyendo también varios ejemplos de pruebas, mantenimientos y/o actualizaciones que puedan haberse realizado en estos años en la empresa ficticia, proveyendo de los documentos de BCP actualizados.

De la misma manera pueden realizarse otras simulaciones similares sobre empresas de otros sectores, donde puedan existir diferentes amenazas y vulnerabilidades, así como diferentes soluciones con las que mitigarlas, que puedan generar otros planes de continuidad distintos a partir de los mismos desarrollos propuestos aquí.

Al ser un mundo en constante evolución, pueden plantearse gran cantidad de trabajos tanto futuros como alternativos. Lo realmente importante es que cualquiera de esos trabajos siempre aportará algo, ya que mientras existan empresas existirán amenazas, vulnerabilidades y formas de paliarlos. Mientras existan empresas, siempre existirán planes de continuidad.

6.- Glosario

- Activo: Bien o derecho propiedad de una empresa, y que aparece reflejado en su contabilidad.
- Amenaza: Fenómeno o condición peligrosa capaz de causar un perjuicio de cualquier índole a la persona u objeto en riesgo.
- B.C.P.: Siglas en inglés de Business Continuity Plan (Plan de Continuidad del Negocio).
- Contingencia: Suceso que, de suceder, afectaría al funcionamiento normal de la organización.
- Continuidad: Permanencia del funcionamiento de la empresa en el tiempo.
- Desastre: Evento no previsto que provoca daños en la infraestructura de la empresa, causando la interrupción de su funcionamiento normal durante un periodo de tiempo.
- D.R.P.: Siglas en inglés de Disaster Recovery Plan. Se refiere al Plan de Recuperación de Desastres del área de Tecnologías de Información de una Compañía.
- Equipo de Contingencia: Personal de la empresa a cargo del desarrollo y ejecución de Plan de Continuidad
- Impacto: Consecuencia de una interrupción en un proceso, servicio o sistema.
- P.R.D.: Siglas de Plan de Recuperación Departamental. En el ejemplo simulado, Plan de Recuperación propio de cada Departamento que compone SPBCP Consulting.
- Procesos: Conjunto de actividades que actúan sobre ciertos elementos de entrada produciendo resultados.
- Riesgo: Probabilidad de que una amenaza explote una vulnerabilidad para provocar un daño.
- Sistemas: Conjunto de recursos informáticos de una compañía.
- T.M.I.: Siglas de Tiempo Máximo de Interrupción. Es el tiempo máximo en el que la Empresa podría prescindir de un proceso crítico con un impacto asumible para el negocio.
- T.R.O.: Siglas de Tiempo de Recuperación Objetivo. Es el tiempo necesario esperado para la recuperación de un proceso crítico de la Empresa en caso de que este proceso haya sufrido una interrupción.
- Vulnerabilidad: Existencia de una debilidad en un sistema o proceso que pueda causar un daño en dicho recurso.

7.- Referencias

- [MAGE-HTP] – MAGERIT - GOBIERNO DE ESPAÑA - http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VVda0_ntmko

- [BACK-HOF] - Backing Up Business-Industry Trend or Event – JIM HOFFER - Health Management Technology, Enero 2001

- [PDC-DEF] - **"Planes de Contingencia: La Continuidad del negocio en las organizaciones"** - Juan Gaspar Martínez - Editorial Díaz de Santos, 2004

- [PREV-RAE] - Diccionario de la Real Academia Española de la Lengua – www.rae.es

- [WIK-BCP] – Wikipedia - https://es.wikipedia.org/

8.- Bibliografía

8.1.- Libros

- **"Planes de Contingencia: La Continuidad del negocio en las organizaciones"** - Juan Gaspar Martínez - Editorial Díaz de Santos, 2004

- **"Seguridad Informática en las Empresas"** - Gonzalo Álvarez y Pedro Pablo Pérez - Mc Graw Hill, Madrid, 2004

8.2.- Revistas

- **"Guía práctica para PYMES: Cómo implantar un plan de continuidad de negocio" –** Observatorio de la seguridad de la información, artículo publicado por Deloitte e INTECO (actual INCIBE), Octubre 2010

8.3.- Páginas o documentos electrónicos en la red

- http://www.disaster-recovery-guide.com/ - Guía en internet para recuperación de desastres, accedido durante 2014

- http://searchdatacenter.techtarget.com/ - Página web dedicada a la seguridad informática, accedido en Septiembre de 2014 y Marzo de 2015

- http://www.businesscontingency.com/ - Página dedicada a la preparación de planes de continuidad, accedido en Septiembre de 2014 y Marzo de 2015

- https://www.incibe.es - Instituto Nacional de Ciberseguridad, accedido en Marzo y Abril de 2015

- http://www.drii.org – Página web del Disaster Recovery Institute, accedido en Junio de 2015

- https://es.wikipedia.org/ - Enciclopedia digital, accedido en varias ocasiones durante 2014 y 2015

- http://itil.osiatis.es/ - Página web conteniendo formación ITIL – accedido en Julio de 2015

- https://www.aguirrenewman.es/buscador/alquiler-y-venta/oficinas/la-florida-edificio-america-ii-a6/la-florida/a6/MADR_008143#.VexhFRHtmko –

Página web de alquiler de oficinas con datos sobre la sede de SBPC Consulting – Accedido en Julio de 2015

- https://www.google.es/maps - Página web de mapas de Google, accedida en Agosto de 2015

- www.pandasecurity.com – Página web de antivirus Panda, accedida durante Agosto de 2015

ANEXO I – Análisis de Impacto al Negocio

SPBCP CONSULTING S.A.

Análisis de Impacto al Negocio

Propietario	Dpto. Sistemas Y Seguridad
Mantenido por	Dpto. Sistemas Y Seguridad
Fecha	02/07/2015
Versión	1.0
Próxima Revisión	Julio 2016

INDICE

1. HISTORIA DEL DOCUMENTO

ELABORADO POR	VERSIÓN	FECHA
Director de Sistemas y Seguridad	1.0	02/07/2015

2. OBJETO DEL DOCUMENTO

Se elabora el presente documento con el objetivo de recoger tanto los posibles riesgos a los que se enfrenta SPBPC Consulting S.A., como el impacto que tendría sobre la Compañía el hecho de que estas amenazas finalmente tuvieran lugar.

Este documento incluye tanto el Análisis de Riesgos preliminar como el Análisis de Impacto al Negocio, y en él se determina la prioridad de recuperación de los procesos críticos de la Compañía en caso de necesidad.

3. ANÁLISIS DE RIESGOS

A continuación se detallan los posibles riesgos a los que se puede enfrentar la Compañía, agrupados según la tipología de los mismos:

- Riesgos Naturales.
- Riesgos Tecnológicos.
- Riesgos causados por errores no intencionados.
- Riesgos causados por acciones deliberadas.

Dichos riesgos ordenados por su clasificación se recogen en la siguiente tabla, indicando para cada uno de ellos la probabilidad de ocurrencia y el perjuicio que podría tener para el Negocio en caso de producirse.

RIESGO	TIPO DE RIESGO	PROBABILIDAD	PERJUICIO	AFECTACION
Fuego	Natural	BAJA	ALTO	Infraestructura / Datos
Inundaciones	Natural	BAJA	ALTO	Infraestructura / Datos
Terremotos	Natural	BAJA	ALTO	Infraestructura
Meteorología adversa	Natural	MEDIA	BAJO	Infraestructura
Epidemias / Plagas	Natural	MEDIA	MEDIO	Personal
Fallo suministro eléctrico	Tecnológico	MEDIA	MEDIO	Infraestructura / Datos
Fallo comunicaciones	Tecnológico	MEDIA	BAJO	Datos
Fallo refrigeración	Tecnológico	BAJO	MEDIO	Sistemas
Fallo hardware	Tecnológico	MEDIA	BAJO	Sistemas
Fallo software	Tecnológico	MEDIA	BAJO	Datos
Errores usuarios	Errores NI	MEDIA	MEDIO	Datos
Errores administrador	Errores NI	BAJA	ALTO	Datos
Errores mantenimiento	Errores NI	BAJA	MEDIO	Sistemas
Errores configuración	Errores NI	BAJA	BAJO	Sistemas
Virus informático	Deliberado	ALTA	MEDIO	Sistemas / Datos
Hackers	Deliberado	MEDIA	ALTO	Sistemas / Datos
Suplantación identidad	Deliberado	BAJA	ALTO	Datos
Fraude	Deliberado	BAJA	ALTO	Datos
Robo información	Deliberado	BAJA	ALTO	Datos
Vandalismo / Robo	Deliberado	BAJA	ALTO	Infraestructura
Terrorismo	Deliberado	BAJA	ALTO	Infraestructura

4. ANÁLISIS DE IMPACTO AL NEGOCIO

Se ha realizado el Análisis de Impacto al Negocio recogiendo los parámetros que se indican a continuación, para cada proceso crítico de la Compañía:

- Nombre del Proceso y Departamento al que pertenece.
- Tiempo Máximo de Interrupción (T.M.I.) para cada proceso.
- Tiempo de Recuperación Objetivo (T.R.O.) para cada proceso. Es el tiempo necesario esperado para la recuperación de un proceso crítico de la Empresa en caso de que este proceso haya sufrido una interrupción.
- Personal mínimo necesario para la ejecución de cada proceso.

La siguiente tabla sintetiza toda la información recogida. El orden de aparición en la tabla establece el nivel de criticidad de cada proceso, y también la prioridad de cada uno de ellos en caso de ser necesaria la recuperación.

DEPT. / PROCESO	T.M.I.	T.R.O.	PERSONAL
Sistemas / Comunicaciones + Datos	36 horas	24 horas	1
Operaciones / Proceso1	36 horas	24 horas	8
Operaciones / Proceso2	36 horas	24 horas	8
Operaciones / Proceso3	48 horas	24 horas	6
Proyectos / Proceso1	36 horas	24 horas	8
Proyectos / Proceso2	36 horas	24 horas	6
Ventas / Proceso1	48 horas	24 horas	1
Administración / Proceso1	36 horas	24 horas	2
Infraestructura / Proceso1	48 horas	24 horas	1
RR.HH. / Proceso1	48 horas	24 horas	2
TOTALES			43

Los detalles de recuperación de cada proceso crítico pueden encontrarse en el Plan de Recuperación Departamental de cada área, y que se encuentran en propiedad de la Dirección de cada Departamento.

5. ACTUALIZACIONES NECESARIAS

Será necesaria la revisión y, en su caso, actualización de este documento, en las situaciones que se describen a continuación:

- Revisión periódica anual.
- Cambios en la ubicación de la sede de SPBCP Consulting S.A.
- Cambios en los posibles riesgos descritos.
- Modificación, adición o supresión de los procesos críticos de la Compañía.

**** FIN DEL DOCUMENTO ****

ANEXO II – Plan De Crisis

SPBCP CONSULTING S.A.

Documento de Plan de Crisis

Propietario	Dpto. Sistemas Y Seguridad
Mantenido por	Dpto. Sistemas Y Seguridad
Fecha	09/07/2015
Versión	1.0
Próxima Revisión	Julio 2016

INDICE

1. HISTORIA DEL DOCUMENTO

ELABORADO POR	VERSIÓN	FECHA
Director de Sistemas y Seguridad	1.0	09/07/2015

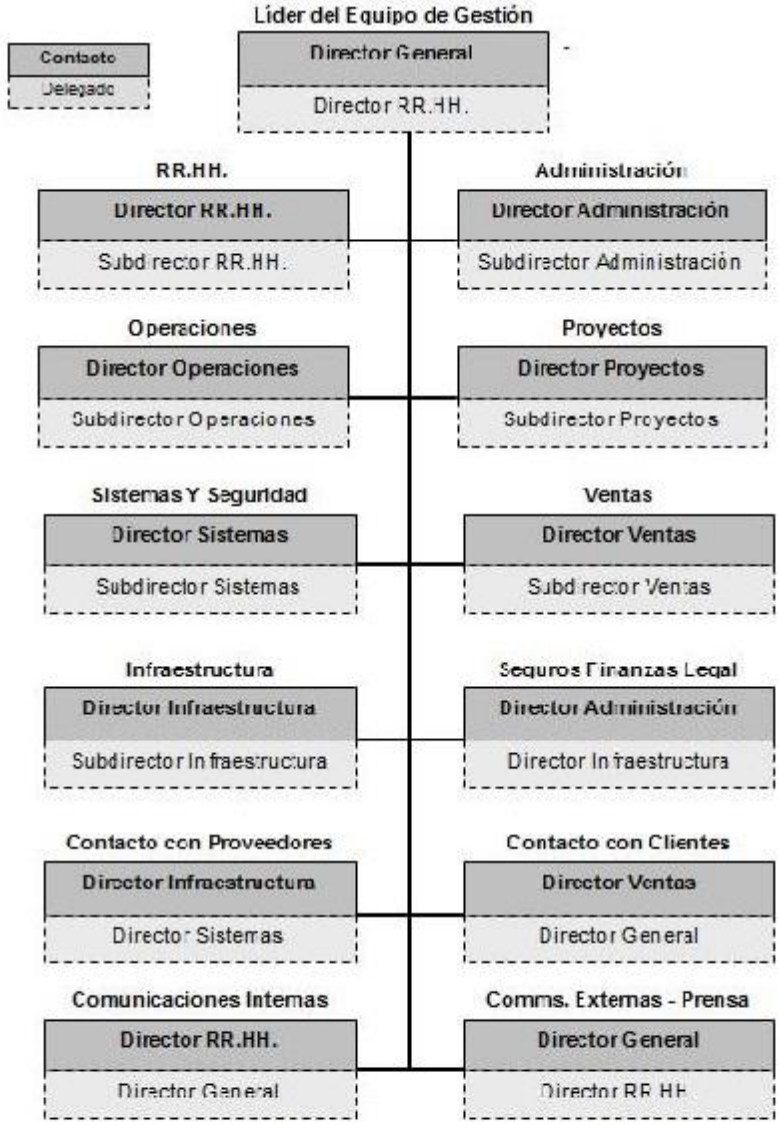
2. OBJETO DEL DOCUMENTO

Se elabora el presente documento con el objetivo de establecer las actuaciones a desempeñar por el Equipo de Gestión de Contimuidad en caso de ser necesaria la ejecución del Plan de Continuidad del Negocio.

En este documento se incluyen los datos de contacto necesarios de los proveedores con los que negociar la obtención de los recursos necesarios para establecer nuevamente la infraestructura necesaria para el funcionamiento de la Compañía.

3. EQUIPO DE GESTIÓN DE CONTINUIDAD

A continuación se detalla el Equipo de Gestión de Continuidad de SPBCP Consulting, junto con sus datos de contacto.



A continuación se indican los datos de contacto de cada uno de los componentes del Equipo de Gestión de Continuidad de SPBCP Consulting:

CONTACTO	TELÉFONO 1	TELÉFONO 2	CORREO ELECTRÓNICO
Director General	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director RR.HH.	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector RR.HH.	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director Administración	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector Administración	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director Operaciones	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector Operaciones	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director Proyectos	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector Proyectos	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director Sistemas	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector Sistemas	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director Ventas	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector Ventas	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director Infraestructura	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector Infraestructura	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es

4. PLAN DE CRISIS

A continuación se describen las acciones a tomar por cada miembro del Equipo de Gestión, indicadas en orden de prioridad.

Estas acciones suponen una guía a seguir para un posible escenario de pérdida total de la infraestructura de SPBCP Consulting S.A., pero se adecuarán a cada situación concreta si fuera necesaria la ejecución del BCP.

ACCIÓN	RESPONSABLE
La persona que decide la ejecución del BCP debe disponer de toda la información posible: - Localización y momento del incidente. - Si existen heridos o víctimas mortales. - Alcance y gravedad de los daños. - Impacto de primer nivel: edificio no accesible, corte eléctrico… - Convocar al Equipo de Gestión de Continuidad.	Líder Equipo Gestión Continuidad
Acciones una vez convocado el Equipo de Gestión de Continuidad: - Si la Oficina no está disponible, cuantificar el posible tiempo de no disponibilidad y buscar lugar de trabajo alternativo para el personal crítico. - Establecer un lugar y fecha para la primera reunión del Equipo. - Informar al resto de empleados para que, cuando sea posible, puedan teletrabajar desde sus domicilios. - Gestión por parte de RR.HH. de la posible existencia de heridos o víctimas mortales.	Equipo de Gestión de Continuidad
Primeras 24 horas: Equipo de Gestión de Continuidad: - Actualizar la información de todos los Departamentos. - Asegurar que las instalaciones de la empresa son seguras y que no se permite el acceso a ninguna persona excepto a las Autoridades Locales o el Equipo de Gestión de Continuidad. - Establecer la mejor forma de comunicación en base a la infraestructura existente. - Organizar estancia en hoteles, caterings, etc.para el Equipo de Gestión de Continuidad. - Establecer reuniones periódicas de actualización.	Equipo de Gestión de Continuidad
Primeras 48 horas: Equipo de Gestión de Continuidad: - Identificar los daños a los activos de la Empresa - Determinar el tiempo de inoperatividad - Determinar si es necesario realizar desvíos telefónicos - Comunicaciónes internas a los empleados - Considerar la necesidad de comunicaciones externas - Si es necesario, buscar ubicación alternativa para lanzar el Plan de Recuperación, dependiendo del tiempo estimado de no disponibilidad de las infraestructuras.	Equipo de Gestión de Continuidad
Primeras 48 horas: Departamento de Infraestructura - Evaluación daños - Búsqueda de lugares alternativos si fuera necesario	Infraestructura

Primeras 48 horas: Departamento de Sistemas y Seguridad: - Evaluación de los daños - Recuperación Comunicaciones - Recuperación Sistemas - Recuperación Datos	Sistemas
Primeras 48 horas: Departamento de Operaciones: - Teletrabajo personal crítico	Operaciones
Primeras 48 horas: Departamento de Proyectos: - Teletrabajo personal crítico	Proyectos
Primeras 48 horas: Departamento de Administración: - Disponibilidad fondos recuperación - Cuantificación económica de daños - Contacto con los seguros - Contacto con proveedores críticos	Administración
Primeras 48 horas: Departamento de Ventas: - Contacto con clientes críticos	Ventas
Primeras 48 horas: Departamento de RR.HH. - Atención a los Empleados - Soporte a las distintas áreas de la Compañía para cubrir las necesidades de recursos humanos.	RR.HH.
Días siguientes: - Reuniones periódicas del Equipo de Gestión - Ejecución de los distintos PRD de cada Departamento - Monitorización del proceso de Recuperación - Objetivo: Restaurar la actividad normal de la Compañía	Equipo de Gestión de Continuidad

Los detalles de recuperación de cada proceso crítico pueden encontrarse en el Plan de Recuperación Departamental de cada área, y que se encuentran en propiedad de la Dirección de cada Departamento.

5. CONTACTO CLIENTES Y PROVEEDORES

En la tabla a continuación se indican los datos de contacto de los proveedores de SPBCP Consulting S.A. que puedan proveer del material necesario para la recuperación de la Empresa en los primeros momentos de la ejecución del BCP.

En cuanto al contacto con los Clientes de SPBCP, por motivos de confidencialidad de datos, contratos e imagen corporativa, el contacto con los mismos siempre se realizará desde la Dirección General o la Dirección de Ventas, no siendo objetivo de este documento.

SERVICIO	PROVEEDOR	PERSONA CONTACTO	TELÉFONO
Propiedad Edificio	Proveedor	Nombre Contacto	N. Teléfono
Vigilante Seguridad	Proveedor	Nombre Contacto	N. Teléfono
Sistemas Antiincendios	Proveedor	Nombre Contacto	N. Teléfono
Sistemas Eléctricos	Proveedor	Nombre Contacto	N. Teléfono
Sistema Alarma	Proveedor	Nombre Contacto	N. Teléfono
Mutua de seguros médicos	Proveedor	Nombre Contacto	N. Teléfono
Póliza seguro	Proveedor	Nombre Contacto	N. Teléfono
Banco	Proveedor	Nombre Contacto	N. Teléfono
Material Oficina	Proveedor	Nombre Contacto	N. Teléfono
Taxi	Proveedor	Nombre Contacto	N. Teléfono
Alquiler Oficinas Alternativas	Proveedor	Nombre Contacto	N. Teléfono
Alquiler equipos electrógenos	Proveedor	Nombre Contacto	N. Teléfono
Alquileres Informáticos	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Telefonía	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Internet 1	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Internet 2	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Hardware	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Software	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Estaciones Trabajo	Proveedor	Nombre Contacto	N. Teléfono
Sistemas Acceso	Proveedor	Nombre Contacto	N. Teléfono
Cámaras Seguridad	Proveedor	Nombre Contacto	N. Teléfono
Mensajería	Proveedor	Nombre Contacto	N. Teléfono

6. ACTUALIZACIONES NECESARIAS

Será necesaria la revisión y, en su caso, actualización de este documento, en las situaciones que se describen a continuación:

- Revisión periódica anual.
- Cambios en la composición o datos de contacto de los miembros del Equipo de Gestión de Continuidad.
- Cambios en la composición o datos de contacto de proveedores.
- Tras la ejecución del Plan de Crisis, se analizarán las acciones tomadas y su adecuación al Plan, modificando, añadiendo o eliminando las acciones existentes según la experiencia obtenida.

**** FIN DEL DOCUMENTO ****

ANEXO III – Disaster Recovery Plan

SPBCP CONSULTING S.A.

DRP Sistemas Y Seguridad

Propietario	Dpto. Sistemas Y Seguridad
Mantenido por	Dpto. Sistemas Y Seguridad
Fecha	16/07/2015
Version	1.0
Próxima revisión	Julio 2016

INDICE

1. HISTORIA DEL DOCUMENTO

ELABORADO POR	VERSIÓN	FECHA
Director de Sistemas y Seguridad	1.0	16/07/2015

2. OBJETO DEL DOCUMENTO

Se elabora el presente documento con el objetivo de indicar los pasos necesarios desde el ámbito del Departamento de Seguridad y Sistemas para reestablecer la operativa normal de la infraestructura informática de SPBCP Consulting S.A., en caso de ser necesaria la ejecución del Plan de Continuidad de Negocio.

3. INVENTARIO

A continuación se detallan el inventario y ubicación actuales de todos los elementos que gestiona y mantiene el Departamento de Sistemas Y Seguridad:

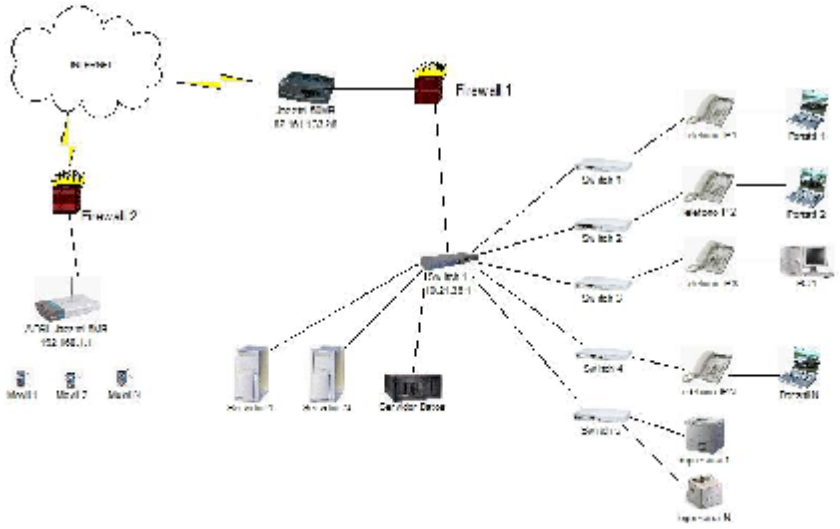
ELEMENTO	MODELO	CANTIDAD	UBICACION
Teléfono Fijo	Cisco IP Phone 6940	160	Oficina
Teléfono Fijo	Cisco IP Phone 6940	12	Stock
Teléfono Móvil	Samsung Galaxy Core	8	Dirección
Teléfono Móvil	Samsung Galaxy Mini	10	Operaciones
Teléfono Móvil	Samsung Galaxy Mini	5	Ventas
Teléfono Móvil	Samsung Galaxy Mini	4	Proyectos
Monitor	Monitor HP 21"	155	Oficina
Monitor	Monitor HP 24"	8	Dirección
Portátil	HP Elitebook 8470p	8	Dirección
Portátil	HP Probook 6460b	87	Operaciones
Portátil	HP Probook 6470b	54	Proyectos
Portátil	HP Probook 6470b	1	Sistemas
Portátil	HP Probook 6470b	5	Ventas
Portátil	HP Probook 6470b	10	Stock
Ordenador	HP Compaq 8000 Elite SFF	3	Administración
Ordenador	HP Compaq 8000 Elite SFF	1	Infraestructura
Ordenador	HP Compaq 8000 Elite SFF	3	RR.HH.
Impresora	Canon IR 2020 Color	2	Operaciones
Impresora	Canon IR 2020 Color	1	Proyectos
Impresora	Canon IR 2020 Color	1	Ventas
Impresora	HP Laserjet 4300	2	Administración
Impresora	HP Laserjet 4300	1	RR.HH.
Modem USB 4G	Modem USB 4G	8	Sistemas
Alarma	Alarma de seguridad	1	Sistemas
Cámaras seguridad	Samsung SND-6011R	4	Sistemas
Control de acceso	Lectores control acceso	3	Sistemas
Videograbador	Samsung SHR-2162N	1	Sistemas
Servidores DHCP/DNS	HP Proliant ML110G5	1	Sistemas
Servidores Apps	HP Proliant DL120	2	Sistemas
Servidor Datos	HP Proliant X 1600	1	Sistemas
Backup syst.	HP StorageWorks Utrium 1760	1	Sistemas
UPS	Smart UPS RT-5000	2	Sistemas
RACKS	APC AR-3100	2	Sistemas
Firewalls	CISCO ASA 5520	2	Sistemas

Switches	CISCO Catalyst 3750G 48 puertos	6	Sistemas
Comms	CISCO 2811 Jazztel	1	Sistemas
Wifi	Linksys CISCO WRT 160	2	Sistemas
HDD USB Backups	Seagate 1 TB	3	Sistemas
Cintas backups	Cintas HP LTO4 Utrium 1.6TB	20	Sistemas

4. MAPA DE CONEXIONES

Se indica a continuación el mapa de conexiones de SPBCP Consulting S.A. Estas conexiones se establecen de la siguiente manera:

- Conexión a Internet de 50MB de fibra óptica provista por Jazztel PLC, para proporcionar la conectividad interna necesaria en la LAN de SPBCP Consulting.
- Conexión ADSL a Internet de 6MB contratada para proporcionar conectividad inalámbrica a los dispositivos móviles corporativos.
- 2 Firewall configurados para proteger las conexiones de la red local al exterior
- Switches de conexión
- 2 servidores de aplicación
- 1 servidor de datos
- 1 sistema de backup por cintas
- Teléfonos IP, estaciones de trabajo, impresoras y escáneres



5. POLÍTICA DE COPIAS DE SEGURIDAD

Para salvaguardar la disponibilidad e integridad de la información, se ha establecido la política de salvaguardas que se indica en este apartado.

ELEMENTO	FRECUENCIA	DISPOSITIVO	UBICACION
Equipos Usuarios	N/A	Servidor Datos < 2 GB	Interna
S.O. Servidor Datos	Semestral	Cintas backup	Interna
Datos Servidor Datos	Semanal	Cintas backup	Interna
S.O. Servidor App1	Semestral	Cintas backup	Interna
S.O. Servidor App2	Semestral	Cintas backup	Interna

6. ACCIONES DE RECUPERACION

A continuación se especifican, ordenadas por orden de prioridad, las acciones necesarias para recuperar la infraestructura informática de SPBCP ante una situación de desastre.

ACCIÓN	DETALLE
Establecer Comunicaciones básicas	Contactar proveedores internet para disponer de conexión básica en el menor tiempo posible. Contactar proveedor de telefonía móvil para proporcionar conectividad de módem / datos móviles a los usuarios críticos.
Establecer Infraestructura básica	Contactar con proveedores de hardware para adquirir la configuración básica necesaria para recuperar los datos de la Compañía – 1 RACK, 1 Servidor App + Datos. Contactar con proveedores de conectividad LAN para establecer la red local necesaria básica (por cable o inalámbrica).
Equipos de Usuario	Contactar con proveedores de hardware (compra o alquiler) para proporcionar a los empleados las herramientas básicas para desarrollar sus funciones.
Recuperación de Sistemas	Recuperación / Instalación de los Sistemas App + Datos .
Recuperación de Datos	Recuperación de datos corporativos desde copia de seguridad.
Recuperación Seguridad	Contacto con proveedores alarmas y sistemas de acceso para establecer una infraestructura básica. Contacto con proveedores de grabación digital para cámaras de seguridad.
Vuelta a normalidad	Ampliar las infraestructuras básicas ya provistas gradualmente hasta conseguir la situación de funcionamiento normal antes del suceso.

7. CONTACTO PROVEEDORES

La siguiente tabla especifica los contactos de los proveedores necesarios para dotar de las conexiones y sistemas mencionados en este documento.

SERVICIO	PROVEEDOR	PERSONA CONTACTO	TELÉFONO
Sistema Alarma	Proveedor	Nombre Contacto	N. Teléfono
Alquileres Informáticos	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Telefonía	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Internet 1	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Internet 2	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Hardware	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Software	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Estaciones Trabajo	Proveedor	Nombre Contacto	N. Teléfono
Cámaras Seguridad	Proveedor	Nombre Contacto	N. Teléfono
Sistemas Acceso	Proveedor	Nombre Contacto	N. Teléfono

8. ACTUALIZACIONES NECESARIAS

Será necesaria la revisión y, en su caso, actualización de este documento, en las situaciones que se describen a continuación:

- Revisión periódica anual.
- Cambios en el inventario.
- Modificaciones en la estructura del mapa de conexiones.
- Modificaciones en las políticas de copias de seguridad.
- Cambios en la composición o datos de contacto de proveedores.
- Tras la ejecución de este procedimiento, se analizarán las acciones tomadas y su adecuación al Plan, modificando, añadiendo o eliminando las acciones existentes según la experiencia obtenida.

**** FIN DEL DOCUMENTO ****

ANEXO IV – Plan de Mantenimiento y Pruebas

SPBCP CONSULTING S.A.

Mantenimiento Y Pruebas del BCP

Propietario	Dpto. Sistemas Y Seguridad
Mantenido por	Dpto. Sistemas Y Seguridad
Fecha	23/07/2015
Versión	1.0
Próxima Revisión	Julio 2016

INDICE

1. HISTORIA DEL DOCUMENTO

ELABORADO POR	VERSIÓN	FECHA
Director de Sistemas y Seguridad	1.0	23/07/2015

2. OBJETO DEL DOCUMENTO

Se ha elaborado el presente documento con el objetivo de establecer las políticas necesarias para el mantenimiento del Plan de Contimuidad del Negocio de SPBCP Consulting S.A., crear un modelo de prueba para el ensayo de dicho Plan, y poseer un registro tanto de las actualizaciones del Plan de Contimuidad del Negocio como de las pruebas realizadas y las acciones correctoras necesarias.

3. MANTENIMIENTO DEL BCP

Las políticas que rigen el mantenimiento del BCP de SPBCP Consulting S.A. se indican a continuación:

- SPBCP Consulting S.A. dispondrá en todo momento de un Plan de Continuidad de Negocio actualizado y realista, que permita garantizar en la medida de lo posible la continuidad del Negocio en caso de desastre.

- Todos los Directores de Departamento, así como el Director General, dispondrán de una copia actualizada de dicho Plan.

- El Departamento de Sistemas Y Seguridad será el propietario del Plan, así como el encargado de su mantenimiento.

- Se realizará una revisión anual periódica del Plan completo, así como de su documentación asociada. Tras esta revisión, si fuera necesario se procederá a actualizar el plan.

- Se realizará una revisión y actualización del Plan y sus documentos asociados si aconteciera alguna o varias de las situaciones a continuación:

    - Ejecución del Plan
    - Modificación de los miembros o datos de contacto del Equipo de Gestión de Continuidad
    - Modificación de las conexiones, sistemas o infraestructura IT.
    - Modificación de los riesgos que afronta la Compañía.
    - Cambios en la ubicación de la Sede de SPBCP Consulting S.A.
    - Modificación de los proveedores o sus datos de contacto.
    - Necesidad de actualización o cambio tras alguna de las pruebas realizadas.

- Con periodicidad anual, se realizará un ejercicio práctico de ejecución del Plan. Este ejercicio planteará una situación simulada que tendrá que ser resuelta por el Equipo de Gestión de Continuidad. Se registrará tanto la situación simulada como las conclusiones tras su realización.

- Con periodicidad anual, se formará a todos los empleados de la Compañía en las particularidades del citado Plan, consiguiendo así su concienciación y colaboración en caso de que fuera necesaria la ejecución del mismo.

4. PRUEBAS

Con periodicidad anual, se realizará una simulación teórico-práctica de una situación ficticia que implique la ejecución del Plan de Continuidad. Se convocará a todo el Equipo de Gestión de la Continuidad y se evaluará la respuesta a la situación de emergencia y cómo está preparada la Compañía para afrontarla.

Tras el ejercicio, se analizarán los resultados, se obtendrán las conclusiones pertinentes y se propondrán las mejoras y actuaciones necesarias a implementar en el Plan de Continuidad.

La tabla a continuación describe un modelo de prueba para el Plan de Continuidad.

EVENTO	IMPACTO	ACCIONES A TOMAR
04:15 – 13 de Octubre de 2015 Fuego en el edificio	*A evaluar por el Equipo de Gestión de Continuidad*	*A rellenar por el Equipo de Gestión de Continuidad*
04:30 – 13 de Octubre de 2015 Acuden los servicios de emergencia	*A evaluar por el Equipo de Gestión de Continuidad*	*A rellenar por el Equipo de Gestión de Continuidad*
05:45 – 13 de Octubre de 2015 Fuego mitigado – Edificio dañado	*A evaluar por el Equipo de Gestión de Continuidad*	*A rellenar por el Equipo de Gestión de Continuidad*
Carretera cortada – no hay posibilidad de llegar al edificio salvo para los equipos de emergencia	*A evaluar por el Equipo de Gestión de Continuidad*	*A rellenar por el Equipo de Gestión de Continuidad*
08:35 – 13 de Octubre de 2015 El edificio no estará disponible el resto del día. Equipos de limpieza y recuperación acceden al lugar.	*A evaluar por el Equipo de Gestión de Continuidad*	*A rellenar por el Equipo de Gestión de Continuidad*
12:15 – 13 de Octubre de 2015 Se han detectado humo y daños estructurales en el edificio	*A evaluar por el Equipo de Gestión de Continuidad*	*A rellenar por el Equipo de Gestión de Continuidad*
16:15 – 13 de Octubre de 2015 Edificio cerrado. Tiempo estimado de cierre para reparaciones: 12 semanas	*A evaluar por el Equipo de Gestión de Continuidad*	*A rellenar por el Equipo de Gestión de Continuidad*
DEFICIENCIAS	**ACCIONES CORRECTORAS**	**FECHA IMPLANTACION**
A rellenar por el Equipo de Gestión de Continuidad	*A rellenar por el Equipo de Gestión de Continuidad*	*A rellenar por el Equipo de Gestión de Continuidad*
A rellenar por el Equipo de Gestión de Continuidad	*A rellenar por el Equipo de Gestión de Continuidad*	*A rellenar por el Equipo de Gestión de Continuidad*
A rellenar por el Equipo de Gestión de Continuidad	*A rellenar por el Equipo de Gestión de Continuidad*	*A rellenar por el Equipo de Gestión de Continuidad*

5. REGISTRO EJERCICIOS BCP

En la tabla a continuación aparece el registro de los ejercicios BCP realizados hasta el momento.

EJERCICIO	FECHA	ASISTENTES	MEDIDAS APLICADAS

6. REGISTRO ACTUALIZACIONES

La tabla a continuación detalla las distintas actualizaciones que se han realizado al Plan de Continuidad de Negocio.

ACCIÓN	FECHA	TIPO REVISIÓN	DOCUMENTOS AFECTADOS
Implantación BCP	Julio 2015	Creación	BCP Completo

**** FIN DEL DOCUMENTO ****

ANEXO V – Business Continuity Plan

SPBCP CONSULTING S.A.

Plan de Continuidad del Negocio

Propietario	Dpto. Sistemas Y Seguridad
Mantenido por	Dpto. Sistemas Y Seguridad
Fecha	30/07/2015
Versión	1.0
Próxima Revisión	Julio 2016

INDICE

1. HISTORIA DEL DOCUMENTO

ELABORADO POR	VERSIÓN	FECHA
Director de Sistemas y Seguridad	1.0	30/07/2015

2. OBJETO DEL DOCUMENTO

El documento a continuación recoge en detalle el Plan de Continuidad de Negocio de SPBCP Consulting S.A.

Este Plan de Continuidad de Negocio detalla el conjunto de análisis, medidas activas y preventivas, pruebas y documentos, y está elaborado con el objetivo de mitigar los efectos adversos de un posible desastre, guiando paso por paso al personal a cargo de la restauración de la actividad de la Compañía desde el momento en que se produzca el evento.

La finalidad última del Plan es la de servir de guía y apoyo en un eventual proceso de recuperación de los procesos del Negocio tras una crisis, en un periodo de tiempo que afecte lo menos posible al cumplimiento de los compromisos y contratos de la misma con sus clientes, para que la crisis ocasione el mínimo impacto posible a la Compañía.

3. ESTRUCTURA DEL BCP

Estratégicamente, SPBCP Consulting S.A. dispondrá en todo momento de un Plan de Continuidad de Negocio actualizado. Este Plan está formado por los siguientes documentos:

- Plan de Continuidad de Negocio (BCP): Un documento que resume todos los aspectos básicos de la Compañía, tales como procesos críticos, datos de contacto, información de la infraestructura de la compañía, etcétera, elaborado para guiar al Equipo de Gestión de Continuidad en la recuperación.

- Plan de Recuperación Departamental (P.R.D.): Son uno o más documentos internos a cada uno de los Departamentos de SPBCP Consulting S.A., que indican para cada área cómo proceder en caso de ser necesaria la recuperación del servicio. Será responsabilidad de cada Departamento el almacenamiento y mantenimiento de cada P.R.D.

- Disaster Recovery Plan (DRP): Documento que especifica la infraestructura de IT de la Compañía, y los pasos necesarios para su recuperación tras una emergencia.

- Plan de Crisis: Documento que indica las acciones a realizar en caso de ser necesaria la ejecución del BCP.

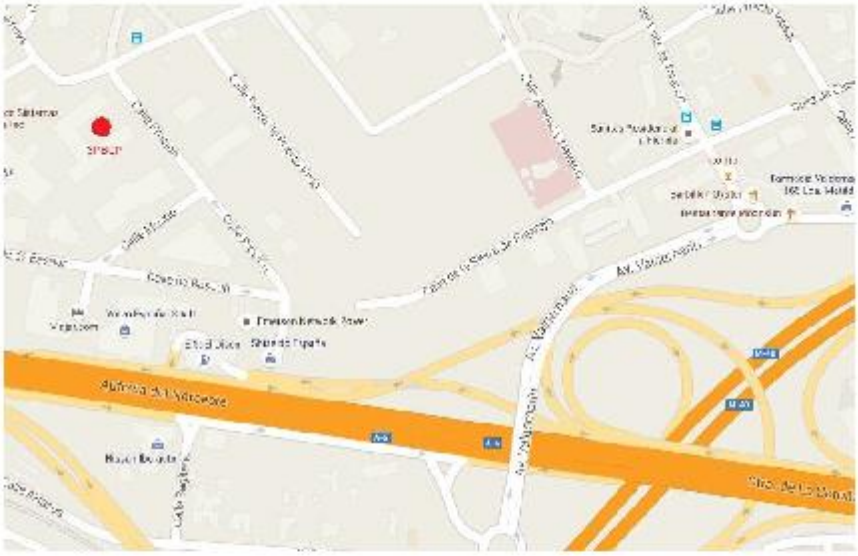
- Plan de Mantenimiento y Pruebas: Documento que resume las políticas de mantenimiento y actualización del Plan. En este documento también se recogen las pruebas y simulaciones realizadas hasta el momento para asegurar la funcionalidad del BCP.

4. SPBCP CONSULTING S.A.

Se describen a continuación las principales características de SPBCP Consulting S.A.

- Razón social: SPBCP Consulting S.A.
- Domicilio social: C\Proción 7, 28023 Madrid
- Actividad de la Empresa: Consultoría informática
- Número de Empleados: 160
- Facturación: Superior a 14.000.000 € anuales

Las oficinas de SPBCP Consulting S.A. están situadas al norte de la ciudad de Madrid, y son fácilmente accesibles por carretera, dada su proximidad a la Autovía del Noroeste - Carretera de La Coruña – A6 y a la circunvalación M-40. Adicionalmente, la ciudad de Madrid dispone de una amplia y variada red de comunicaciones, y es fácilmente accesible por carretera, avión o ferrocarril, y dispone de numerosas infraestructuras tales como trenes de cercanías, metro, metro ligero o autobuses.



La Compañía se encuentra ubicada en el Edificio América II, que cuenta con medidas de seguridad y prevención propias tales como sistema anti-incendios, acceso restringido, sistema de alarma, vigilante de seguridad, cámaras de seguridad, etcétera.

En la tabla a continuación se describen los riesgos a los que está expuesta la Compañía, tanto por su ubicación como por la naturaleza de su negocio:

RIESGO	TIPO DE RIESGO	PROBABILIDAD	PERJUICIO	AFECTACION
Fuego	Natural	BAJA	ALTO	Infraestructura / Datos
Inundaciones	Natural	BAJA	ALTO	Infraestructura / Datos
Terremotos	Natural	BAJA	ALTO	Infraestructura
Meteorología adversa	Natural	MEDIA	BAJO	Infraestructura
Epidemias / Plagas	Natural	MEDIA	MEDIO	Personal
Fallo suministro eléctrico	Tecnológico	MEDIA	MEDIO	Infraestructura / Datos
Fallo comunicaciones	Tecnológico	MEDIA	BAJO	Datos
Fallo refrigeración	Tecnológico	BAJO	MEDIO	Sistemas
Fallo hardware	Tecnológico	MEDIA	BAJO	Sistemas
Fallo software	Tecnológico	MEDIA	BAJO	Datos
Errores usuarios	Errores NI	MEDIA	MEDIO	Datos
Errores administrador	Errores NI	BAJA	ALTO	Datos
Errores mantenimiento	Errores NI	BAJA	MEDIO	Sistemas
Errores configuración	Errores NI	BAJA	BAJO	Sistemas
Virus informático	Deliberado	ALTA	MEDIO	Sistemas / Datos
Hackers	Deliberado	MEDIA	ALTO	Sistemas / Datos
Suplantación identidad	Deliberado	BAJA	ALTO	Datos
Fraude	Deliberado	BAJA	ALTO	Datos
Robo información	Deliberado	BAJA	ALTO	Datos
Vandalismo / Robo	Deliberado	BAJA	ALTO	Infraestructura
Terrorismo	Deliberado	BAJA	ALTO	Infraestructura

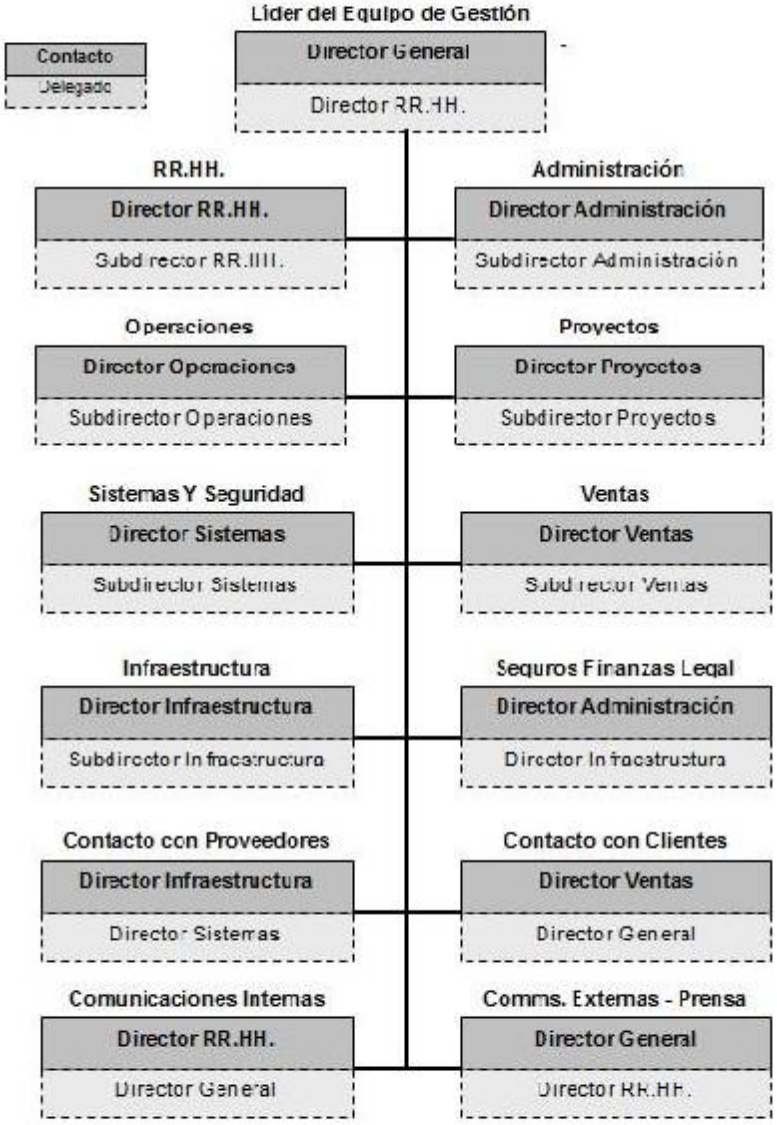
Las medidas de seguridad implantadas por la Compañía para hacer frente a los riesgos mencionados anteriormente se detallan en la tabla a continuación:

ELEMENTO	DESCRIPCIÓN	RESPONSABLE
Detectores Humo	10 detectores de humo	Infraestruct.
Extintores	10 extintores	Infraestruct.
Sistema eléctrico	Protecciones y fases diferenciadas	Infraestruct.
Botiquín	Primeros auxilios	RR.HH.
Vigilante de seguridad	Vigilante 24x7	Edificio
Alarma	5 detectores movimiento + centralita	Sistemas
Cámaras de seguridad	4 cámaras + grabador	Sistemas
Control de acceso electrónico	4 lectores acceso + software	Sistemas
Acceso usuarios a sistemas	Acceso protegido por contraseña	Sistemas
Seguridad equipos	Antivirus corporativo	Sistemas
Seguridad servidores	Acceso restringido Sistemas	Sistemas
Seguridad de red	Firewalls	Sistemas
Copia seguridad servidores aps.	Semestral Cinta de almacenamiento	Sistemas
Copia seguridad servidor datos	Semanal Cinta de almacenamiento	Sistemas
Sistema UPS racks	2 UPS / 30 minutos	Sistemas
Políticas de seguridad informática para empleados	Políticas por escrito firmadas por todos los empleados	RR.HH.
Seguros	Cobertura empleados y material	RR.HH.

En la tabla a continuación se muestra la organización de SPBPC Consulting S.A. a nivel departamental:

DEPARTAMENTO	RESPONSABLE	CONTACTO	NUMERO EMPLEADOS
Dirección General	Nombre Apellidos	N. Teléfono	1
RR.HH.	Nombre Apellidos	N. Teléfono	4
Administración	Nombre Apellidos	N. Teléfono	4
Operaciones	Nombre Apellidos	N. Teléfono	88
Proyectos	Nombre Apellidos	N. Teléfono	53
Sistemas	Nombre Apellidos	N. Teléfono	2
Ventas	Nombre Apellidos	N. Teléfono	6
Infraestructura	Nombre Apellidos	N. Teléfono	2

SPBCP Consulting S.A. ha establecido el siguiente Equipo de Gestión de Continuidad, que liderará la recuperación de la Compañía en caso de ser necesaria la ejecución de este Plan:



A continuación se indican los datos de contacto de cada uno de los componentes del Equipo de Gestión de Continuidad de SPBCP Consulting:

CONTACTO	TELÉFONO 1	TELÉFONO 2	CORREO ELECTRÓNICO
Director General	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director RR.HH.	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector RR.HH.	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director Administración	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector Administración	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director Operaciones	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector Operaciones	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director Proyectos	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector Proyectos	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director Sistemas	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector Sistemas	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director Ventas	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector Ventas	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Director Infraestructura	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es
Subdirector Infraestructura	N. Teléfono	N. Teléfono	Nombre.apellido@spbpc.es

5. RECUPERACIÓN

A pesar de las medidas de prevención implementadas, puede darse el caso de que parte o la totalidad de las infraestructuras, sistemas o recursos de la SPBCP Consulting no estén operativos y no sea posible la ejecución de los procesos críticos de la Compañía, con el consiguiente impacto para el Negocio.

Los mencionados procesos críticos son mostrados en la siguiente tabla, en relación con el personal mínimo necesario para llevarlos a cabo, el tiempo necesario para la recuperación (T.R.O.) y el tiempo máximo de interrupción asumible (T.M.I.):

DEPT. / PROCESO	T.M.I.	T.R.O.	PERSONAL
Sistemas / Comunicaciones + Datos	36 horas	24 horas	1
Operaciones / Proceso1	36 horas	24 horas	8
Operaciones / Proceso2	36 horas	24 horas	8
Operaciones / Proceso3	48 horas	24 horas	6
Proyectos / Proceso1	36 horas	24 horas	8
Proyectos / Proceso2	36 horas	24 horas	6
Ventas / Proceso1	48 horas	24 horas	1
Administración / Proceso1	36 horas	24 horas	2
Infraestructura / Proceso1	48 horas	24 horas	1
RR.HH. / Proceso1	48 horas	24 horas	2
TOTALES			**43**

A continuación se describen las acciones necesarias para recuperar los procesos críticos de la Compañía con un impacto asumible. Estas acciones suponen una guía a seguir para un posible escenario de pérdida total de la infraestructura de SPBCP Consulting S.A., pero se adecuarán a cada situación concreta en que fuera necesaria la ejecución del BCP.

ACCIÓN	RESPONSABLE
La persona que decide la ejecución del BCP debe disponer de toda la información posible: - Localización y momento del incidente. - Si existen heridos o víctimas mortales. - Alcance y gravedad de los daños. - Impacto de primer nivel: edificio no accesible, corte eléctrico… - Convocar al Equipo de Gestión de Continuidad.	Líder Equipo Gestión Continuidad
Acciones una vez convocado el Equipo de Gestión de Continuidad: - Si la Oficina no está disponible, cuantificar el posible tiempo de no disponibilidad y buscar lugar de trabajo alternativo para el personal crítico. - Establecer un lugar y fecha para la primera reunión del Equipo. - Informar al resto de empleados para que, cuando sea posible, puedan	Equipo de Gestión de Continuidad

teletrabajar desde sus domicilios. - Gestión por parte de RR.HH. de la posible existencia de heridos o víctimas mortales.	
Primeras 24 horas: Equipo de Gestión de Continuidad: - Actualizar la información de todos los Departamentos. - Asegurar que las instalaciones de la empresa son seguras y que no se permite el acceso a ninguna persona excepto a las Autoridades Locales o el Equipo de Gestión de Continuidad. - Establecer la mejor forma de comunicación en base a la infraestructura existente. - Organizar estancia en hoteles, caterings, etc.para el Equipo de Gestión de Continuidad. - Establecer reuniones periódicas de actualización.	Equipo de Gestión de Continuidad
Primeras 48 horas: Equipo de Gestión de Continuidad: - Identificar los daños a los activos de la Empresa - Determinar el tiempo de inoperatividad - Determinar si es necesario realizar desvíos telefónicos - Comunicaciónes internas a los empleados - Considerar la necesidad de comunicaciones externas - Si es necesario, buscar ubicación alternativa para lanzar el Plan de Recuperación, dependiendo del tiempo estimado de no disponibilidad de las infraestructuras.	Equipo de Gestión de Continuidad
Primeras 48 horas: Departamento de Infraestructura - Evaluación daños - Búsqueda de lugares alternativos si fuera necesario	Infraestructura
Primeras 48 horas: Departamento de Sistemas y Seguridad: - Evaluación de los daños - Recuperación Comunicaciones - Recuperación Sistemas - Recuperación Datos	Sistemas
Primeras 48 horas: Departamento de Operaciones: - Teletrabajo personal crítico	Operaciones
Primeras 48 horas: Departamento de Proyectos: - Teletrabajo personal crítico	Proyectos
Primeras 48 horas: Departamento de Administración: - Disponibilidad fondos recuperación - Cuantificación económica de daños - Contacto con los seguros - Contacto con proveedores críticos	Administración
Primeras 48 horas: Departamento de Ventas: - Contacto con clientes críticos	Ventas
Primeras 48 horas: Departamento de RR.HH. - Atención a los Empleados - Soporte a las distintas áreas de la Compañía para cubrir las necesidades de recursos humanos.	RR.HH.
Días siguientes: - Reuniones periódicas del Equipo de Gestión - Ejecución de los distintos PRD de cada Departamento - Monitorización del proceso de Recuperación - Objetivo: Restaurar la actividad normal de la Compañía	Equipo de Gestión de Continuidad

Los detalles de recuperación de cada proceso crítico pueden encontrarse en el Plan de Recuperación Departamental de cada área, y que se encuentran en propiedad de la Dirección de cada Departamento.

6. DISASTER RECOVERY PLAN (D.R.P.)

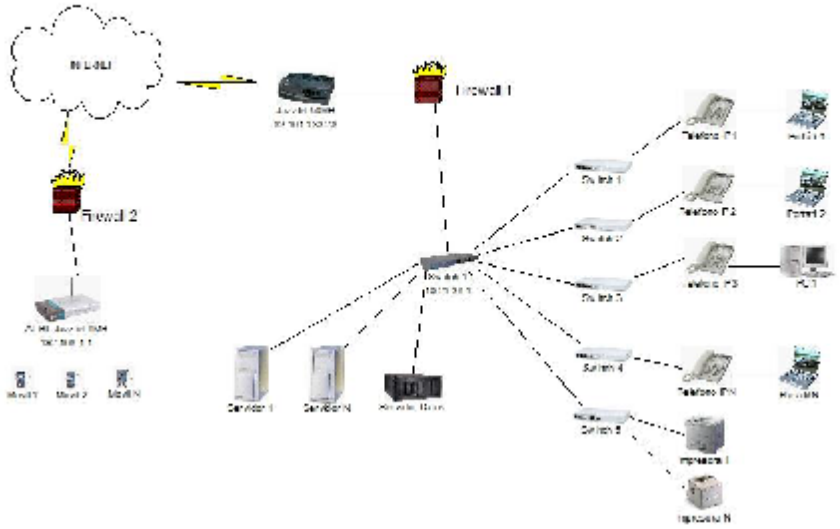
Este apartado incluye el Plan Departamental de Recuperación del Departamento de Sistemas y Seguridad, que indica cómo recuperar la infraestructura de IT de la Compañía. A pesar de ser un documento independiente y propio del Departamento de Sistemas y Seguridad, se incluye en este documento dada la criticidad de dicha infraestructura informática para toda la Compañía.

En primer lugar, se detalla el inventario de los distintos Sistemas de SPBCP Consulting, incluyendo características generales y modelos por si fuera necesario su reemplazo:

ELEMENTO	MODELO	CANTIDAD	UBICACION
Teléfono Fijo	Cisco IP Phone 6940	160	Oficina
Teléfono Fijo	Cisco IP Phone 6940	12	Stock
Teléfono Móvil	Samsung Galaxy Core	8	Dirección
Teléfono Móvil	Samsung Galaxy Mini	10	Operaciones
Teléfono Móvil	Samsung Galaxy Mini	5	Ventas
Teléfono Móvil	Samsung Galaxy Mini	4	Proyectos
Monitor	Monitor HP 21"	155	Oficina
Monitor	Monitor HP 24"	8	Dirección
Portátil	HP Elitebook 8470p	8	Dirección
Portátil	HP Probook 6460b	87	Operaciones
Portátil	HP Probook 6470b	54	Proyectos
Portátil	HP Probook 6470b	1	Sistemas
Portátil	HP Probook 6470b	5	Ventas
Portátil	HP Probook 6470b	10	Stock
Ordenador	HP Compaq 8000 Elite SFF	3	Administración
Ordenador	HP Compaq 8000 Elite SFF	1	Infraestructura
Ordenador	HP Compaq 8000 Elite SFF	3	RR.HH.
Impresora	Canon IR 2020 Color	2	Operaciones
Impresora	Canon IR 2020 Color	1	Proyectos
Impresora	Canon IR 2020 Color	1	Ventas
Impresora	HP Laserjet 4300	2	Administración
Impresora	HP Laserjet 4300	1	RR.HH.
Modem USB 4G	Modem USB 4G	8	Sistemas
Alarma	Alarma de seguridad	1	Sistemas
Cámaras seguridad	Samsung SND-6011R	4	Sistemas
Control de acceso	Lectores control acceso	3	Sistemas
Videograbador	Samsung SHR-2162N	1	Sistemas
Servidores DHCP/DNS	HP Proliant ML110G5	1	Sistemas
Servidores Apps	HP Proliant DL120	2	Sistemas

Servidor Datos	HP Proliant X 1600	1	Sistemas
Backup syst.	HP StorageWorks Utrium 1760	1	Sistemas
UPS	Smart UPS RT-5000	2	Sistemas
RACKS	APC AR-3100	2	Sistemas
Firewalls	CISCO ASA 5520	2	Sistemas
Switches	CISCO Catalyst 3750G 48 puertos	6	Sistemas
Comms	CISCO 2811 Jazztel	1	Sistemas
Wifi	Linksys CISCO WRT 160	2	Sistemas
HDD USB Backups	Seagate 1 TB	3	Sistemas
Cintas backups	Cintas HP LTO4 Utrium 1.6TB	20	Sistemas

El mapa de conexiones de red de la Compañía se muestra a continuación:



La tabla a continuación recoge las políticas de salvaguarda de los servidores de la Compañía:

ELEMENTO	FRECUENCIA	DISPOSITIVO	UBICACION
Equipos Usuarios	N/A	Servidor Datos < 2 GB	Interna
S.O. Servidor Datos	Semestral	Cintas backup	Interna
Datos Servidor Datos	Semanal	Cintas backup	Interna
S.O. Servidor App1	Semestral	Cintas backup	Interna
S.O. Servidor App2	Semestral	Cintas backup	Interna

Se han definido las acciones a continuación en caso de ser necesaria una recuperación de la infraestructura de IT:

ACCIÓN	DETALLE
Establecer Comunicaciones básicas	Contactar proveedores internet para disponer de conexión básica en el menor tiempo posible. Contactar proveedor de telefonía móvil para proporcionar conectividad de módem / datos móviles a los usuarios críticos.
Establecer Infraestructura básica	Contactar con proveedores de hardware para adquirir la configuración básica necesaria para recuperar los datos de la Compañía – 1 RACK, 1 Servidor App + Datos. Contactar con proveedores de conectividad LAN para establecer la red local necesaria básica (por cable o inalámbrica).
Equipos de Usuario	Contactar con proveedores de hardware (compra o alquiler) para proporcionar a los empleados las herramientas básicas para desarrollar sus funciones.
Recuperación de Sistemas	Recuperación / Instalación de los Sistemas App + Datos .
Recuperación de Datos	Recuperación de datos corporativos desde copia de seguridad.
Recuperación Seguridad	Contacto con proveedores alarmas y sistemas de acceso para establecer una infraestructura básica. Contacto con proveedores de grabación digital para cámaras de seguridad.
Vuelta a normalidad	Ampliar las infraestructuras básicas ya provistas gradualmente hasta conseguir la situación de funcionamiento normal antes del suceso.

7. CONTACTO CLIENTES Y PROVEEDORES

En la tabla a continuación se indican los datos de contacto de los proveedores de SPBCP Consulting S.A. que puedan proveer del material necesario para la recuperación de la Empresa en los primeros momentos de la ejecución del BCP.

En cuanto al contacto con los Clientes de SPBCP, por motivos de confidencialidad de datos, contratos e imagen corporativa, el contacto con los mismos siempre se realizará desde la Dirección General o la Dirección de Ventas, no siendo objetivo de este documento.

SERVICIO	PROVEEDOR	PERSONA CONTACTO	TELÉFONO
Propiedad Edificio	Proveedor	Nombre Contacto	N. Teléfono
Vigilante Seguridad	Proveedor	Nombre Contacto	N. Teléfono
Sistemas Antiincendios	Proveedor	Nombre Contacto	N. Teléfono
Sistemas Eléctricos	Proveedor	Nombre Contacto	N. Teléfono
Sistema Alarma	Proveedor	Nombre Contacto	N. Teléfono
Mutua de seguros médicos	Proveedor	Nombre Contacto	N. Teléfono
Póliza seguro	Proveedor	Nombre Contacto	N. Teléfono
Banco	Proveedor	Nombre Contacto	N. Teléfono
Material Oficina	Proveedor	Nombre Contacto	N. Teléfono
Taxi	Proveedor	Nombre Contacto	N. Teléfono
Alquiler Oficinas Alternativas	Proveedor	Nombre Contacto	N. Teléfono
Alquiler equipos electrógenos	Proveedor	Nombre Contacto	N. Teléfono
Alquileres Informáticos	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Telefonía	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Internet 1	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Internet 2	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Hardware	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Software	Proveedor	Nombre Contacto	N. Teléfono
Proveedor Estaciones Trabajo	Proveedor	Nombre Contacto	N. Teléfono
Sistemas Acceso	Proveedor	Nombre Contacto	N. Teléfono
Cámaras Seguridad	Proveedor	Nombre Contacto	N. Teléfono
Mensajería	Proveedor	Nombre Contacto	N. Teléfono

8. ACTUALIZACIONES NECESARIAS

Será necesaria la revisión y, en su caso, actualización de este documento, en las situaciones que se describen a continuación:

- Tras la ejecución del Plan. En esta situación se analizarán las acciones tomadas y su adecuación al Plan, y se modificará el Plan de acuerdo con la experiencia obtenida.
- Modificación de los miembros o datos de contacto del Equipo de Gestión de Continuidad.
- Modificación de los datos de los diferentes Departamentos.
- Modificación de las conexiones, sistemas o infraestructura IT.
- Modificación del Inventario tecnológico de la Compañía.
- Modificación de los riesgos que afronta la Compañía.
- Cambios en la ubicación de la Sede de SPBCP Consulting S.A.
- Modificación de los proveedores o sus datos de contacto.
- Necesidad de actualización o cambio tras alguna de las pruebas realizadas.

El siguiente registro muestra todas las modificaciones llevadas a cabo en el BCP:

ACCIÓN	FECHA	TIPO REVISIÓN	PARTES AFECTADAS
Implantación BCP	Julio 2015	Creación	BCP Completo

**** FIN DEL DOCUMENTO ****